Guía para costurar patrones de defensa de los derechos humanos en el entorno digital

Registrando incidentes de seguridad digital como práctica de mitigación del riesgo

Zurciendo
Comunicación
Cultura Digital

Registrando incidentes de seguridad digital como práctica de mitigación del riesgo

Guía para costurar patrones de defensa de los derechos humanos en el entorno digital

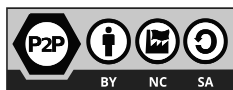
AGRADECIMIENTOS

A Valentina Caprotti de SweFOR por su asesoría en materia de seguridad integral. A Flor Goldsman periodista y ciberfeminista, a Omar Valencia de la Cooperativa Tierra Común y a Anamhoo de Técnicas Rudas por los comentarios a la catalogación de incidentes.

CRÉDITOS

Coordinación: Valentina Auletta
Textos: Valentina Auletta, dom, la_jes
Catalogación de incidentes: la_jes, Valentina Auletta, dom, xolotl
Edición: dom
Diseño editorial y maquetación: Irene Soria Guzmán
Esta investigación fue realiza por Sursiendo con el apoyo del Fondo de Respuesta Rápida gestionado por la organización Derechos Digitales, con el aporte financiero de la Fundación Ford.

Escrito, editado y diseñado con software libre.



Índice

0.- Introducción 5

1.- Capítulo uno. Metro en mano: Midiendo el riesgo y la amenaza digital 13
- 1.1.- América Latina Vigilada 23
- 1.2.- Más allá de la información 27
- 1.3.- Ecuación de riesgo en lo digital 18
- 1.4.- Análisis de amenazas 20
  - 1.4.1.- Análisis de incidentes de seguridad 21
  - 1.4.2.- Mapeo de actores 22
  - 1.4.3.- Análisis de contexto 22
  - 1.4.4.- Actualizar, resguardar, mapear 23

2.- Capítulo 2. Deshilachando los incidentes de seguridad digital 27
- 2.1.- El proceso de Registro de Incidentes de seguridad digital 32
  - 2.1.1.- Identificar los ISD 33
  - 2.1.2.- Documentar los ISD 36
  - 2.1.3.- Catalogar los ISD 38
  - 2.1.4.- Analizar los ISD 41

3.- Conclusiones. Cierres y vueltas 45

4.- Anexo. Categorización de Incidentes de Seguridad Digital 51

5.- Glosario 65

6.- Referencias 71

Registrando incidentes de seguridad digital como práctica de mitigación del riesgo. Guía para costurar patrones de defensa de los derechos humanos en el entorno digital.

Sursiendo, 2020

Sursiendo, Comunicación y Cultura Digital somos una organización dedicada al trabajo en torno a las tecnologías de internet nacida en mayo de 2011 en Chiapas, México. Somos un pequeño grupo de personas que tenemos como ejes temáticos la comunalidad digital, los derechos digitales colectivos y los hackfeminismos. Todo ello a través de una participación equitativa y creativa que pone en el centro una perspectiva de género, apoyándonos en la educación popular y el software libre. En nuestros trayectos también nos relacionamos con procesos de defensa de derechos humanos y de la tierra y el territorio.

Introducción

"Si bien la llegada de Internet y las redes sociales presagiaba una democratización del acceso a la información y la comunicación, en particular para los defensores y las defensoras, numerosos dispositivos de vigilancia, reglamentación y represión se han desarrollado en el transcurso de los últimos años, a menudo para limitar la participación política y social de los titulares de derechos y de las personas quienes los defienden"
(Michel Forst, 2020: 24)

Los colectivos, grupos y organizaciones que defienden derechos humanos estamos cada vez más conscientes de la necesidad de cuidarnos de los riesgos que supone esta labor. La violencia en nuestra contra proviene hoy de instituciones estatales, agentes de seguridad del Estado, actores empresariales, grupos armados, e incluso de miembros de nuestras mismas comunidades, y se perpetra a través de diversas estrategias y escalas.

Cuidar la integridad física ya no basta, hoy también se pone atención a las dimensiones psicosocial, digital, pero también espiritual, económica y de género, así como a sus intersecciones. Por ello en el campo de la seguridad y protección de activistas y personas que defienden derechos humanos en las últimas dos décadas, asistimos a la expansión del concepto de seguridad, bajo la premisa de que se trata de un fenómeno subjetivo, que afecta de manera diferente a cada quien de acuerdo a las estructuras de dominación que nos atraviesan, vinculado a un contexto y coyuntura específicos.

Lo anterior ha llevado a la creciente integración del ámbito de la seguridad física y organizacional con el de la seguridad digital, tanto en la producción conceptual como en el abordaje práctico. En particular, organizaciones referentes en el ámbito de la seguridad y protección de

El concepto de seguridad digital preferimos transformarlo en el de Cuidados Digitales Colectivos

activistas y personas defensoras de derechos humanos (Brigadas Internacionales de Paz, 2014; Protección Internacional, 2009; Front Line Defenders; 2016) han posicionado "la seguridad" como una triada conformada por la seguridad física, la seguridad psicosocial o emocional y la seguridad digital. Solo actuando sobre estas tres dimensiones al mismo tiempo es posible expandir y mantener espacios abiertos para la defensa de los derechos humanos.

Lo anterior es compartido también por quienes han dedicado sus esfuerzos a mejorar la seguridad digital de activistas y advierten que "centrarse exclusivamente en la seguridad digital puede ignorar el cuadro completo y dar como resultado consejos de seguridad redundantes o dañinos" (The Engine Room, 2018:12). La organización Tactical Tech es quien adopta por primera vez de manera explícita un enfoque de "seguridad holística" que "en lugar de mirar por separado la importancia de nuestra seguridad digital, de nuestro bienestar psicosocial, y de los procesos de seguridad organizacional busca integrarlos y evidenciar sus interrelaciones" (2016:11).

Si bien Sursiendo comparte este enfoque integral, "consideramos que la 'seguridad' como concepto es en sí mismo engañoso y ha desembocado en el estado de vigilancia en el que cual estamos actualmente. No hay manera posible de estar 'seguras y seguros' al 100%, pero sí podemos tomar medidas para cuidar nuestras acciones digitales y así cuidar también nuestro trabajo de defensoría y activismos" (Sursiendo; 2019:9).

El concepto de seguridad digital preferimos transformarlo en el de ***Cuidados Digitales Colectivos***, con el cual describimos el conjunto de prácticas de protección que los sujetos colectivos, entendidos aquí como grupos, colectivos, organizaciones o redes que defienden derechos humanos, ideamos y construimos a diferente escala para cuidarnos mutuamente y así prevenir y mitigar el riesgo, solucionar problemas concretos, y mejorar nuestra 'vida digital' en un largo camino hacia la autonomía tecnológica.

En ese sentido coincidimos con aquellas perspectivas que ven el cuidado "como un acto de auto-preservación subversivo y político, que es fundamental para volver efectivas la estrategia y cultura de seguri-

dad" (Tactical Tech, 2016:12). Un cuidado que desde la perspectiva de Sursiendo debe ser colectivo, por lo tanto mutuo, ya que, como afirma el representante de una de las organizaciones que acompañamos todo lo que "tiene una implicación en cuanto a la seguridad, involucra al equipo completo, tiene que ser en un acuerdo discutido" (Nataniel Hernández del Centro de Derechos Humanos Digna Ochoa, 2020).

Una de las prácticas de Cuidados Colectivos que ha tenido más relevancia entre los sujetos colectivos que defienden derechos humanos en América Latina es la de poner atención a los ***Incidentes de Seguridad.*** Estos son entendidos como "cualquier hecho o acontecimiento que pensamos podría afectar a nuestra seguridad personal o como organización" (Protección Internacional, 2009:47). Esta práctica permite identificar patrones de ataques en nuestra contra perpetrados por quienes se oponen a nuestro trabajo, pero también riesgos del contexto en el que nos desenvolvemos o vulnerabilidades internas, y en base a ello proponer acciones que nos fortalezcan.

Si en el campo de los Cuidados Integrales se trata de una práctica ya relativamente arraigada, aunque reciente, en el de los Cuidados Digitales es más bien incipiente. Algunas razones identificadas responden a que gran parte de los incidentes de seguridad digital no "pasan por el cuerpo", por lo tanto no son vistos como una amenaza tangible; lo digital es en ocasiones difícil de diagnosticar o investigar, por lo que entender qué pasó muchas veces implica la intervención de una persona técnica; y el descubrimiento de nuevos tipos de ataques sucede por lo regular gracias a filtraciones (por ejemplo los softwares de espionaje dirigidos, muy complejos de rastrear).

Aún así, reconocemos algunos pasos adelante: por un lado, a lo interno de colectivos y grupos que defienden derechos humanos se empiezan a registrar los incidentes de seguridad digital como práctica de protección colectiva, impulsada especialmente por organizaciones que se dedican al acompañamiento en seguridad y protección y/o a la seguridad digital de terceros, a través de talleres y otras iniciativas. Por otro, se han impulsado servicios de atención y respuesta a incidentes de terceros, como es el caso del "Observatorio Centroamericano de Seguridad Digital", creado por Fundación Acceso (2019), que busca visibilizar las

Cuidarnos mutuamente y así prevenir y mitigar el riesgo, solucionar problemas concretos, y mejorar nuestra 'vida digital' en un largo camino hacia la autonomía tecnológica

prácticas de agresión vigentes en el ámbito digital y que cierran el espacio para la defensa de Derechos Humanos en Centroamérica o la Línea de Ayuda en Seguridad Digital de Access Now (2019) que proporciona respuestas de emergencia y asesoría a individuos y colectivos que han sufrido ataques digitales por defender derechos humanos.

A lo largo de los años en Sursiendo hemos apoyado fortalecer sus Cuidados Digitales Colectivos a otras organizaciones y colectivos del Sureste de México y Centroamérica. Al principio a través de talleres puntuales, charlas y otras actividades no consecutivas, hasta reconocer la necesidad de impulsar procesos de acompañamiento integral de largo plazo, diseñados a partir de las necesidades de los sujetos colectivos involucrados. Así en 2018 arrancamos nuestro primer proceso de Acompañamiento en Seguridad Digital.

La primera tarea que nos propusimos fue realizar un diagnóstico, que culminó con la publicación del Informe "Investigación sobre seguridad digital con organizaciones sociales de Chiapas". A partir de los hallazgos de éste, en 2019 conformamos un equipo interdisciplinario y dimos inicio al acompañamiento como tal, a los talleres, al soporte técnico y al seguimiento personalizado e integral a cinco organizaciones que defienden y promueven los derechos humanos, en particular los derechos de las mujeres, de las personas migrantes y de los pueblos indígenas en sus luchas por la equidad, la tierra y la vida.

En este camino nos dimos cuenta de que los Incidentes de Seguridad Digital son una realidad cotidiana para quienes defienden derechos humanos, que no solo entorpecen su trabajo diario sino que pueden causar daños y afectaciones, poner en riesgo a las personas y al colectivo en su conjunto, o cerrar espacios para la labor de defensa que desempeñan.

Aun en un contexto periférico como el de Chiapas, donde la brecha tecnológica es grande, registramos tanto incidentes que responden a ataques directos, como la intervención telefónica, la difamación e intimidación en redes sociales como incidentes que muestran las vulnerabilidades internas de las organizaciones y las criticidades del entorno en el que se desempeñan, por ejemplo, la pérdida o el robo de información, y la actividad inusual de dispositivos, programas y aplicaciones.

Aprendimos que todos ellos son indicadores importantes de los niveles de amenaza que enfrentan las organizaciones y colectivos que defienden derechos humanos y nos brindan luces acerca del camino a emprender para mitigar las vulnerabilidades y potenciar las capacidades internas. Sin embargo, observamos con preocupación dos tendencias: la de ignorar o poner poca atención a estos incidentes porque son demasiados, abruman, o en todo caso no se sabe qué hacer con ellos, y, por otro lado, la de delegar su abordaje a terceros, normalmente personas técnicas.

Con la mochila cargada de la inspiración que nos proveen las organizaciones y colectivos que trabajan en favor de la justicia social, de los valiosos aportes de quienes se han especializado en fortalecer las prácticas de protección para defender los derechos humanos y los aprendizajes de nuestro propios caminos, proponemos entonces la **Herramienta para el Registro de Incidentes de Seguridad Digital** acompañada de la presente Guía. Son dos insumos con los que buscamos apoyar a grupos, colectivos y redes que defienden derechos humanos y fortalecer sus prácticas de **Cuidados Digitales Colectivos**, en ese camino hacia la autonomía tecnológica. Tenemos el convencimiento de que entender, registrar y analizar nuestros propios incidentes de seguridad digital nos puede llevar a tener más consciencia acerca de nuestras capacidades y límites, dirigir acciones para mejorar nuestra seguridad, tener mayor preparación ante nuevos ataques y compartir aprendizajes con otros y otras. Con esta publicación buscamos facilitar esa tarea.

Buscamos apoyar a grupos, colectivos y redes que defienden derechos humanos y fortalecer sus prácticas de Cuidados Digitales Colectivos, en ese camino hacia la autonomía tecnológica

La **Herramienta de Registro de Incidentes de Seguridad Digital** es el corazón de nuestra propuesta, y está pensada para que sean los mismos grupos quienes puedan ordenar sus Incidentes de Seguridad Digital, catalogarlos, tipificarlos y emprender un primer nivel de análisis. Si es alimentada con regularidad, además de proporcionarles un mapa de lo que acontece en materia de seguridad a lo interno de su organización y colectivo, en determinado arco de tiempo, les dotará de elementos descriptivos y analíticos, que les permitirán reaccionar a los incidentes de la manera más adecuada, les ayudará en sus sesiones de análisis de seguridad así como en el diseño de medidas específicas de protección.

Herramienta y Guía están dirigidos a sujetos colectivos que defienden derechos humanos en América Latina

Quisimos acompañar la Herramienta de esta **Guía para el Registro de Incidentes de Seguridad Digital**, que profundice las razones por las cuales el registro de Incidentes de Seguridad Digital es una práctica fundamental de Cuidados Digitales Colectivos y facilite su uso.

Herramienta + Guía están dirigidos a sujetos colectivos que defienden derechos humanos en América Latina, se preocupan por sus cuidados colectivos y tienen inquietud por fortalecerlos en el aspecto digital. En particular resultará útil a aquellas organizaciones que acompañan a personas, colectivos o procesos de base y que por ello almacenan y comparten información sensible de terceros.

Quienes tengan ya un ejercicio regular de registro y análisis de Incidentes del ámbito físico encontrarán el uso del Herramienta + Guía relativamente sencillo e intuitivo, pero también están pensados para ser usados por parte de quienes se enfrentan a esa práctica de protección por vez primera. Si bien ambos instrumentos buscan incentivar que la tarea de análisis de incidentes se realice de manera autónoma dentro de los equipos de trabajo, estamos conscientes en algunos casos esta instancia será insuficiente y se precisará contar con el apoyo de una persona técnica para el análisis de las tecnologías afectadas.

La guía está estructurada de la siguiente manera:

El capítulo 1. Metro en mano: Midiendo el riesgo y la amenaza digital, ahonda en la importancia del Registro de Incidentes de Seguridad Digital como etapa del análisis de amenaza, práctica imprescindible para fortalecer los Cuidados Digitales Colectivo de grupos, colectivos y organizaciones que defienden derechos humanos. En él aprenderemos **por qué** poner atención a los ISD.

El capítulo 2. Deshilachando los incidentes de seguridad digital, es el instructivo que les acompañará en el proceso de llenado de la "Herramienta", a través de preguntas generadoras y tablas de clasificación. En él aprenderemos **qué** son los incidentes de seguridad digital, **para qué** y **cómo** registrarlos.

Las Conclusiones esbozan los pasos que siguen a la acción del registro, para empezar a pensar en **qué viene después**.

Capítulo uno

Metro en mano: Midiendo el riesgo y la amenaza digital

"La seguridad electrónica y privacidad digital deben convertirse no solo en un área importante para la comprensión y la participación, sino también en un nuevo campo de batalla en la lucha por la adhesión a los principios de la Declaración Universal en todo el mundo" (Front Line Defenders, 2016:10)

En el presente capítulo analizamos brevemente la situación de amenaza digital que sufren quienes defienden derechos humanos en América Latina, lo que nos permitirá aclarar la perspectiva desde la cual en Sursiendo miramos hacia los Incidentes de Seguridad Digital.

Introduciremos además la ecuación de riesgo, instrumento que tomamos prestado del campo de la seguridad integral, explicaremos cómo ésta se aplica a lo digital para finalmente ubicar el Registro de Incidentes de Seguridad Digital en la tarea más amplia de análisis de amenaza.

1.1.- América Latina vigilada

En un mundo cada vez más digitalizado, América Latina es la región donde más ha aumentado la población que se conecta a Internet en los últimos años, pasando de 52% en 2015 a 69% en 2020, según Internet World Stats.

En esta situación, la información (es decir, los datos) es el bien más preciado: quien más consigue recopilar, usar y analizar, más poder tiene,

reflejado en mayores beneficios económicos y mayor control social. Nunca antes el dicho la "información es poder" se ha ajustado más a la realidad.

Tres sectores principales son quienes buscan obtener la mayor cantidad de datos posible para ser usados en perjuicio de la población conectada: las corporaciones tecnológicas, los organismos gubernamentales y la ciberdelincuencia. Pero también es usual encontrarse con grupos y personas "comunes" que reproducen las estructuras de violencia existente a través de medios digitales.

Normalmente, en las notas e informes publicados por medios o gobiernos suelen aparecer incidentes digitales relacionados con intrusiones a las redes empresariales o de instituciones, que mencionan nombres técnicos y las pérdidas económicas que conllevan. Lo que no suelen aparecer son informaciones sobre ataques a organizaciones y personas defensoras de derechos humanos, sino solo algunos relacionados con la delincuencia para crear cierta alarma social.

Menos aún suelen aparecer informaciones sobre el uso que hacen las corporaciones tecnológicas de los datos personales de millones de personas, que al comerciar con ellos, obtienen grandes beneficios económicos y políticos.

Es usual encontrarse con grupos y personas "comunes" que reproducen las estructuras de violencia existente a través de medios digitales

En el caso de la vigilancia, los últimos años hemos visto que algunas instituciones y organismos han cruzado la línea de la legalidad para hacer una utilización abusiva de los datos, a la hora de recopilarlos y usarlos. Y más en un contexto en el que "las fuerzas armadas han ganado influencia política considerable" (Flores-Macías, 2020).

Por eso nos proponemos hacer una breve recopilación de algunos incidentes de seguridad digital ocurridos en los últimos años en América Latina en contra de quienes defienden derechos humanos:

- Violencia machista a través de redes digitales. En todos los países de América Latina existe el ejercicio de la violencia machista a través de dispositivos y programas. Y más aún en contra de defensoras de derechos humanos. Hacemos mención al caso de El Salvador, donde se da

la alerta de organizaciones preocupadas por incremento de violencia digital en contra de defensoras (IM-Defensoras, 2020).

• En México, el #GobiernoEspía. La campaña con ese nombre que iniciaron varias organizaciones sociales tenía como fin denunciar prácticas opacas y violatorias de derechos humanos haciendo uso de las tecnologías, especialmente con la inyección de un malware espía llamado Pegasus contra periodistas y defensores de derechos humanos. Ya había sucedido algo parecido en años anteriores con el caso FinFisher (Sursiendo, 2019a).

• En 2018 se conoció en Chile la Operación Huracán, con la que los Carabineros realizaban **montajes policiales** contra dirigentes mapuches. Durante el operativo en 2017, la fuerza de seguridad expuso presuntos **mensajes** de las aplicaciones Whatsapp y Telegram de los comuneros en los que coordinaban acciones violentas, por lo que procedieron a detenerlos de **forma preventiva** . Posteriormente, las pericias realizadas por el Ministerio Público determinaron que los teléfonos incautados **habían sido intervenidos** por organismos de inteligencia de Carabineros para incluir conversaciones en sus respectivos grupos de mensajería, pruebas obtenidas supuestamente tras la incautación de sus celulares (Wikipedia, 2019).

• Vigilancia en Argentina: a inicios de 2020 se divulgó una lista de 500 periodistas, integrantes de organizaciones sociales y académicos vigilados y fichados por la Agencia Federal de Inteligencia (AFI) en años anteriores, durante la presidencia de Mauricio Macri. Muchos fueron evaluados por su trabajo como “peligros potenciales para la seguridad y el régimen constitucional”, según se ha podido leer en las pocas fichas a las que se ha tenido acceso. También se han realizado deportaciones y vigilancia contra personas de la oposición política y de movimientos sociales, supuestamente por intervención de correos. Así salió a la luz una práctica ilegítima e ilegal de control social (CELS, 2017; Cibeira, 2020).

• Las respuestas de gobiernos a las masivas protestas sociales que se desarrollaron durante 2019 en Colombia, Bolivia, Chile y Ecuador: se utilizaron distintas tecnologías digitales en favor de la represión, criminalización y persecución de las y los manifestantes y su legítimo dere-

cho a reunirse y expresarse pacíficamente, de una manera que solamente puede ser definida como antidemocrática y contraria a los derechos fundamentales. Sobre todo se hizo a través del monitoreo y uso de las redes sociales, ubicación, requisado de dispositivos, etc. (Sursiendo, 2019b).

• Al igual que como ocurrió en otros países, Proyecto de Ley sobre desinformación presentado por el gobierno brasileño a mediados de 2020 amenaza la libertad de expresión y la privacidad en línea. Según organizaciones locales que están siguiendo el tema (The Intercept Brasil Live, 2020) existen en el texto formas de abusos en la criminalización de prácticas comunes, definiciones amplias y extensivas, y requisitos de identificación que amenazan la privacidad y la libertad de expresión, y generan nuevas formas de discriminación. Por ejemplo, propone la obligación de identificación por medio de documentos de identidad y un número único de teléfono celular para el uso de las redes y amplía las obligaciones de retención de datos preexistentes para permitir el monitoreo del reenvío de información en aplicaciones de mensajería (Sursiendo, 2020).

• En Honduras se lanzó a inicios de 2020 una iniciativa de Ley que Regula los Actos de Odio y Discriminación en Redes Sociales e Internet, que propone la censura de contenido considerado como discriminatorio, de odio, injuria, amenaza o incitación a la violencia. Sin embargo, no menciona los parámetros para determinar qué contenido entra dentro de estas consideraciones y debe ser bloqueado, dejando en mano de empresas privadas, a menudo extranjeras, el poder de evaluar qué contenido es ilegal y la obligación de tomar decisiones de censura, cuando estas son facultades que, en un país democrático, corresponden a los tribunales de justicia (Sursiendo, 2018).

• Persecución a investigadores de seguridad digital, allanamiento de domicilios, incautación de equipos informáticos, a veces con acusaciones falsas y desproporcionadas. Les vigilan, detienen e inician proceso judicial sin pruebas suficientes. Ejemplos: los casos de Ola Bini en Ecuador (EFF, 2019) y Javier Smaldone en Argentina (Sursiendo, 2019c).

• En todo el continente se han producido ataques a periodistas independientes y personas defensoras de derechos humanos, a través de las redes digitales o apoyándose en ellas para agredirles posteriormente.

Los mecanismos de transparencia y rendición de cuentas son indispensables para mejorar el ejercicio de derechos. Sin embargo, la historia nos demuestra que éstos nunca son suficientes y que las instancias de poder, tanto públicas como privadas, cometen abusos contra derechos humanos cada vez que pueden. Por eso, sin descuidar las acciones de incidencia que se realizan, nuestras apuestas se enfocan en fortalecer capacidades locales y colectivas.

1.2.- Más allá de la información

Los casos mencionados antes son tan solo una pequeña muestra de los niveles de amenaza digital que sufrimos quienes defendemos derechos humanos en la región. A su vez nos revelan que si bien la información es el primer blanco de la vigilancia, los medios digitales permiten a quienes quieren causarnos daños u obstaculizar la defensa de derechos humanos afectar a nuestros datos y a la vez comprometer nuestras esferas emocionales, económicas, físicas y organizativa, ya que el mundo digital, lejos de ser un mero contenedor de información, abarca hoy casi todos los ámbitos de la vida.

Por lo anterior, en Sursiendo optamos por un enfoque integral, que nos permita dirigir nuestras prácticas de Cuidados Digitales Colectivos hacia la protección de nuestra integridad común, poniendo atención a nuestras prácticas, equipos y dispositivos, a nuestras comunicaciones y navegación, a nuestra imagen pública y a nuestra información.

Los mecanismos de transparencia y rendición de cuentas son indispensables para mejorar el ejercicio de derechos

Quienes defendemos derechos humanos solemos tener sobrecarga de trabajo, nuestras actividades de promoción y defensa ocupan gran parte de nuestros días y al mismo tiempo implementar medidas, planes y rutinas que nos protejan de cualquier ataque es muy complejo. Por ello, creemos que nuestras acciones de Cuidados Digitales Colectivos deben

basarse sobre análisis específicos que nos permitan valorar los niveles de riesgo que enfrentamos y priorizar nuestros esfuerzos con base a ello.

Los riesgos a los que nos enfrentamos son subjetivos y están íntimamente ligados al contexto en el que nos movemos, a nuestras características internas y a los intereses que "tocan" nuestras acciones. Todos ellos son elementos que cambian rápidamente e imponen que los análisis sean regulares y/o ligados a acontecimientos específicos.

1.3. Ecuación de riesgo en lo digital

Uno de los instrumentos que nos ayuda en la valoración de nuestros niveles de riesgo y nos permite identificar los elementos sobre los que podemos incidir para mitigarlo es la **ecuación de riesgo,** ampliamente reconocida y aplicada en el ámbito de la seguridad integral:

riesgo = amenazas x vulnerabilidades / capacidades[1]

donde las amenazas son componentes externos, mientras que las capacidades y las vulnerabilidades componentes internos a nuestro colectivo, organización o grupo de personas que defienden derechos humanos.

Los riesgos a los que nos enfrentamos son subjetivos y están íntimamente ligados al contexto en el que nos movemos

Si bien la ecuación de riesgo es válida tanto para el entorno físico como para el digital, es preciso hacer unas especificaciones que nos ayuden a comprender qué implicaciones tiene cada uno de sus componentes en este segundo ámbito.

Con **amenazas digitales** nos referimos a hechos, eventos, circunstancias o declaraciones que indican la posibilidad de que suframos daños individuales o colectivos a través de medios o dispositivos digitales.

[1] Ésta ha sido formulada en 2009 por Protección International en su Manual de Protección a Defensores de Derechos Humanos a partir de la adaptación de Van Brabant, Koenraad (2000): Operational Security Management in Violent Environments. Good Practice Review 8. Humanitarian Practice Network. Overseas Development Institute, London.

Pueden ser provocadas con la intención de causarnos daño y obstaculizar nuestra labor de defensa o ser el producto del contexto en el que nos desenvolvemos.

En lo digital, las amenazas se relacionan con intentos de controlar la información que producimos, almacenamos o transmitimos, de obstaculizar nuestras labores de comunicación y navegación, de dañar nuestros equipos, nuestra imagen pública y/o nuestra integridad. En ese caso, se habla de **amenazas dirigidas**. Éstas pueden ser perpetradas por personas físicas o a través de dispositivos y aplicaciones que infectan nuestros dispositivos. Entre las amenazas dirigidas se distinguen las **amenazas directas**, es decir, las que notamos de primera mano, de las **amenazas indirectas**, de las cuales nos enteramos a través de terceras partes, ya sean anuncios, filtraciones o investigaciones.

Las **amenazas no dirigidas** o **contextuales** se relacionan con el entorno en el cual nos movemos, tanto en lo físico como en lo digital. En ese último deben tomarse en cuenta los servicios comerciales que usamos como páginas web, correo electrónicos o redes sociales, que por sus características exponen nuestra información a terceros. Como señala Front Line Defenders: "A diferencia de las amenazas que se presentan en el mundo físico, las amenazas digitales a veces son difíciles de notar y, por lo tanto, de prevenir. Con los ataques electrónicos hay tendencia a comportarse de una manera más reactiva que proactiva: esta conducta resulta muchas veces ineficaz" (Front Line Defenders, 2016:15).

Con **vulnerabilidades digitales** nos referimos al daño que pueden provocar las amenazas digitales a nuestra persona, imagen pública, equipos, información, comunicaciones, navegación. En lo digital específicamente las vulnerabilidades se relacionan a menudo con el desconocimiento de ciertas tecnologías, con el descuido o la falta de atención a rutinas de cuidados de la información, de equipos y aplicaciones, o con el uso de ciertos canales de comunicación y navegación no seguros.

Con **capacidades digitales** nos referimos a aquel entramado de aprendizajes, estrategias, instrumentos y rutinas de cuidados que nos hacen más fuertes frente a las amenazas digitales, y disminuyen el impacto de

éstas sobre nuestras personas, equipos y procesos. En lo digital específicamente nos referimos a las rutinas de almacenamiento, respaldo y transmisión de la información, a la elección de determinados equipos, sistemas operativos, software y aplicaciones, a las prácticas de capacitación interna pero también a terceras personas, en particular personas técnicas a quienes podemos acudir en caso de un ataque.

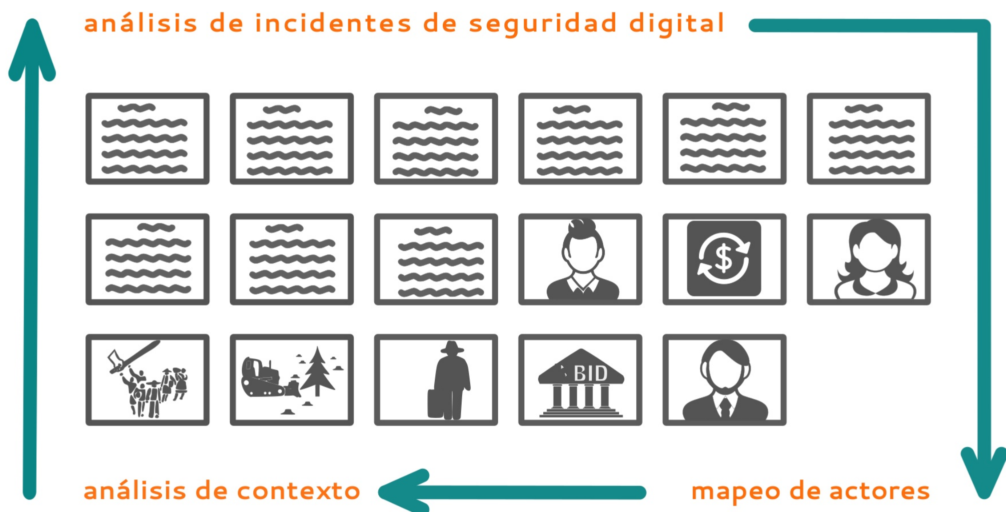
1.4.- Análisis de amenazas

Reconocer las amenazas y darles el justo peso, es decir, valorar qué posibilidades reales tienen de volverse efectivas, es una de las tareas más importantes para poder encauzar nuestros esfuerzos de cuidados colectivos tanto en lo físico como en lo digital, y a la vez cuidar nuestro bienestar emocional. Quienes defendemos derechos humanos estamos a menudo bajo presión por la labor que realizamos y las amenazas buscan abrumarnos, generar paranoia e inmovilizarnos.

Las amenazas, como el riesgo, son dinámicas, cambian de acuerdo al contexto y a los intereses de nuestros oponentes: “Las amenazas ante las cuáles nos preparamos hoy, pueden llegar a ser irrelevantes en un mes, y la clave para ser ágiles es renovar y refinar nuestras prácticas de seguridad de manera continua” (Tactical Tech, 2016:56).

Desde el campo de la seguridad integral se han conceptualizado distintas propuestas de ruta para llevar a cabo el análisis de amenazas. Señalamos en particular las publicaciones de Protección Internacional (2009; 2020); Brigadas Internacionales de Paz (2014; 2017) y Front Line Defenders (2011). Todas ellas sugieren llevar a cabo los análisis de manera regular y colectiva, con todas las personas que integran nuestros grupos y organizaciones, apoyándose en documentación fiable y pertinente.

Lo que proponemos desde Sursiendo es la siguiente **ruta de análisis de amenazas,** que integra las anteriores conceptualizaciones con los aprendizajes de nuestro propio caminar:



ESQUEMA 1. ANÁLISIS DE AMENAZA

1.4.1.- Análisis de incidentes de seguridad

Esta etapa tiene el objetivo de identificar las amenazas específicas que ha sufrido nuestra organización en un período determinado. Prevé analizar los incidentes de seguridad del campo físico y del campo digital de los que hemos sido objeto, tanto a nivel individual como colectivo, que han sido previamente registrados y catalogados. Lo anterior permitirá identificar las amenazas concretas que se han presentado, valorar su periodicidad de aparición y repetición, distinguir las amenazas dirigidas de las no dirigidas, identificar patrones de ataques, o los principales actores perpetradores, así como vincular las amenazas a nuestras acciones de defensa de derechos humanos.

El análisis de incidentes de seguridad es una práctica de protección relativamente arraigada en el campo físico, en cambio, en relación a lo digital, aún se tiende a analizar los incidentes de manera individual, uno por uno, tarea realizada muchas veces por una persona técnica experta.

Es importante en particular identificar aquellos aliados de los actores oponentes que se mueven en el ámbito de la tecnología y las telecomunicaciones

Analizar la suma de incidentes acontecidos en determinado período, de manera conjunta por todo el equipo de trabajo involucrado permite identificar de forma más efectiva tendencias y patrones y así planificar estrategias de cuidados digitales colectivos pertinentes que se sumen a acciones de cuidados físicos.

Entre las metodologías existentes para analizar los incidentes de seguridad sugerimos consultar la guía "Cuidándonos" de Protección Internacional (2020:39), y la Guía de Facilitación del Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos de Peace Brigades International (2014:57-59).

Para realizar análisis de incidentes exhaustivo y pertinente se debe partir de una práctica regular de registro, razón por la cuál el siguiente capítulo de la Guía se enfoca en "cómo registrar los Incidentes de Seguridad Digital".

1.4.2.- Mapeo de actores

Esta etapa busca identificar los intereses, recursos y motivaciones de los actores que están detrás de las amenazas en nuestra contra, así como sus redes. Nos referimos a las personas, instituciones y grupos cuyos intereses se ven afectados por nuestro trabajo de defensa de los derechos humanos y que por ello buscan reducir nuestro espacio de actuación. Se realiza a partir de los actores perpetradores identificados en el análisis de incidentes y se puede realizar por niveles, desde lo local pasando por lo nacional hasta llegar a lo internacional.

Para valorar las amenazas digitales este mapeo deberá tener en consideración las capacidades técnicas y los recursos de los actores oponentes, que les permiten desatar ataques que vulneran nuestra información, dispositivos y comunicaciones. Es importante en particular identificar aquellos aliados de los actores oponentes que se mueven en el ámbito de la tecnología y las telecomunicaciones.

Para metodologías de mapeo de actores sugerimos consultar la guía "Cuidándonos" de Protección Internacional (2020:40-41), y el "Manual de Seguridad Holística" de Tactical Techonolgy Collective (2016:64-71).

1.4.3.- Análisis de contexto

Esta etapa busca identificar las amenazas específicas del contexto donde se desarrolla nuestra labor de defensa de derechos humanos y que no están necesariamente dirigidas en nuestra contra. Existen muchas formas para llevarlo a cabo. Se puede proceder por niveles desde lo local, hasta lo internacional, pasando por lo nacional, o analizar las esferas económica, social, política, legal y ambiental por partes. Es importante colocar los actores opositores a nuestro trabajo que se identificaron en el mapeo en el contexto, ubicando sus alianzas.

Para valorar las amenazas digitales es importante que el análisis de contexto tome en consideración aquellas tendencias, cambios legislativos y políticas que van en detrimento de la libertad de expresión y de la privacidad, que despenalicen la vigilancia y la criminalización de quienes difunden información sobre violaciones a derechos humanos.

Para metodologías de análisis de contexto sugerimos acudir a "Tejidos de Protección" del Colectivo Ansur (2013:33-35), "Violaciones, derechos humanos y contexto: herramientas propuestas para documentar e investigar. Manual de Análisis de contexto para casos de Violaciones a los Derechos Humanos" de Flacso México y IBHARI (2017) y al "Manual de Seguridad Integral" de Jane Barry (2011:36).

1.4.4.- Actualizar, resguardar, mapear

Aun con una práctica regular y efectiva de análisis, las amenazas no se pueden prever por completo y tampoco se puede estar siempre alerta frente a ellas, pero la manera en que éstas impactan sobre nuestros cuerpos, emociones y nuestra labor de defensa dependerá de qué tanta atención pongamos en nuestras capacidades y vulnerabilidades, para poder llegar a potenciar las primeras y reducir las segundas.

En lo digital esta tarea no siempre es sencilla, pues los programas usados para la vigilancia van aumentando sus alcances y sofisticación, además de que a menudo quienes defendemos derechos humanos tenemos equipos desactualizados, sistemas operativos privativos más inseguros o sencillamente no sabemos por dónde empezar a fortalecernos, con lo que parece

una tarea imposible de realizar. Sin embargo no hay que desanimarse: la protección digital es un proceso paso a paso y con cada uno estamos protegiendo una capa de nuestra integridad digital.

Entre las medidas preventivas que podemos tomar están las dirigidas a proteger nuestra información, nuestros equipos y dispositivos, nuestras aplicaciones, nuestra imagen pública, nuestra comunicación y navegación de posibles amenazas, ya sean o no dirigidas. Encontramos: rutinas de actualización, herramientas específicas de seguridad digital, y políticas de resguardo y transmisión de la información.

En los últimos años se han producido diversas publicaciones, manuales y guías, que dan algunas pistas para emprender este proceso. Existen las que buscan mitigar las vulnerabilidades más recurrentes detectadas en los grupos que defienden derechos humanos y proporcionan rutinas, prácticas y herramientas, como es el caso de “Security in a Box”, un compendio de herramientas y tácticas editadas por Tactical Technology Collective y Front Line Defenders (2015) o el “Kit de primeros auxilios digitales”, de CiviCert (2020). Otras se concentran más en herramientas, software y aplicaciones para mejorar nuestras capacidades, como la Guía de Autoprotección Digital Contra La Vigilancia, de la Electronic Frontier Foundation (EFF, s/f). Tactical Technology Collective (2015) por su parte ha elaborado una guía dirigida específicamente a mujeres y personas trans que defienden derechos humanos: “Zen y el arte de que la tecnología trabaje para ti", enfocada “hacia la toma de conciencia, el desarrollo de estrategias y de tácticas” de autocuidados digitales, mientras que el colectivo HACK*BLOSSOM propone una “Guía de Seguridad Digital para Feministas Autogestivas” (s/f).

Desde Sursiendo encontramos que todas estas guías son útiles para empezar a fortalecer capacidades digitales. Sin embargo, es importante recordar que las guías no son “recetas” y es por ello que seguir pasos de análisis de nuestra situación, mapeo y contexto son indispensables para encontrar la mejor manera de enfocarnos en lo que necesitamos. En el mejor de los casos, es importante contar con el acompañamiento de un grupo u organización que trabaje en torno a la seguridad digital, aunque esto no sea posible en todos los contextos.

En relación a las vulnerabilidades, un ejercicio muy útil para valorarlas en el campo digital es mapear nuestra información con el objetivo de ordenar toda la que producimos, almacenamos y comunicamos en una escala de más a menos sensible, e identificar aquellos dispositivos, aplicaciones, y software por los que nuestra información circula. Obtendremos con ello un espectro claro para empezar a trabajar en el cuidado de nuestra información sensible.
Si quieren lanzarse en esta tarea les sugerimos acudir al "Mapeo de Información" de Técnicas Rudas (2018) o a la metodología propuesta por la Guía de Facilitación del Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos de Brigadas Internacionales de Paz (2014).

Una vez ejercitadas, comprendidas y adaptadas a nuestro contexto, las prácticas de protección descritas en los apartados anteriores, deberían entrar a formar parte de nuestras estrategias, protocolos y planes de cuidados colectivos. Solo así se garantizará su ejecución regular, asignándoles una o más personas responsables, tiempos y recursos específicos, y asegurándose de evaluar periódicamente los resultados que permiten alcanzar.

Es importante recordar que las guías no son "recetas" y es por ello que seguir pasos de análisis de nuestra situación, mapeo y contexto son indispensables para encontrar la mejor manera de enfocarnos en lo que necesitamos

Capítulo dos

Deshilachando los incidentes de seguridad digital

“Ahora detectamos más incidentes, pero no quiere decir que aumentaron, sino que antes no los veíamos. Se aumentó la capacidad y estamos más atentas a lo que sucede, no tan fácil lo tomamos como algo normal, sino que ya preguntamos, ya cuestionamos, lo compartimos” Integrante del Centro de Derechos de la Mujer de Chiapas (CDMCH), 2020

Después de haber ubicado el registro de incidentes de seguridad digital en el proceso más amplio de análisis de riesgos y amenazas, ha llegado el momento de adentrarnos en esta práctica de protección. En este capítulo entenderemos qué son los Incidentes de Seguridad Digital (ISD), para qué y cómo registrarlos, qué tipología podemos usar para su catalogación y qué pasos dar para empezar a analizarlos. Esto nos permitirá replicar la práctica de Registro de Incidentes de Seguridad Digital a lo interno de nuestros colectivos, organizaciones y grupos e incorporarla a nuestra maleta de Cuidados Digitales Colectivos.

Un Incidente de Seguridad Digital (ISD) es cualquier hecho, evento, circunstancia o declaración, contenida en tecnología digital, que ha provocado algún daño y/o pensamos pueda afectar nuestra integridad individual o colectiva por defender derechos humanos.

Los IDS no son únicamente aquellos provocados por ataques externos, sino que pueden ser internos, producto de un descuido, una desatención o desconocimient o de nuestra parte

Para entenderlo mejor vamos a desentrañar la definición:

- Los ISD no son solamente **hechos delimitados**, sino que abarcan **anomalías** que se repiten en el tiempo, **situaciones** que rodean una persona o un grupo y **enunciaciones** contenidas en medios digitales. En ese sentido son de considerarse ISD, por ejemplo, los errores frecuentes de conexión a la red de internet en nuestras oficinas, afirmaciones de odio o agresivas en nuestra contra en redes sociales o episodios repetidos de pérdida de información de nuestros dispositivos extraíbles, como usb o discos duros.

- Los ISD pueden ser **hechos sospechados** o **verificados**, es decir, que pueden ser **amenazas ya comprobadas**, como mensajes de extorsión que recibimos en nuestros correos electrónicos, pero también **sucesos o declaraciones que no entendemos por completo,** y que desconocemos si pueden llegar a afectarnos. En ese sentido, caben aquí errores de funcionamiento en nuestra página web, que nos impiden comunicarnos pero que aún no conocemos las causas. Éstos bien podrían ser un ataque dirigido u otro tipo de error técnico de los que somos responsables.

- Los ISD pueden provocarnos **daños inmediatos**, como la destrucción de nuestros dispositivos o la pérdida de información, así como **afectaciones de mediano plazo**, como por ejemplo: miedo, preocupación o daños a nuestra imagen pública y credibilidad, que a la larga cierran nuestro espacio de defensa de los derechos humanos. A la vez, los ISD pueden elevar nuestros niveles de amenaza y llegar a comprometer acciones de mitigación del daño que ya teníamos previstas. Por ejemplo, cuando al pasar por un retén miembros de las fuerzas de seguridad nos piden inspeccionar nuestro teléfono celular aunque sea por unos minutos, podríamos ser objeto de infección por malware, hecho que invalidaría medidas de prevención como la encriptación del dispositivos y/o de sus aplicaciones, o el uso de servicios de mensajería seguros.

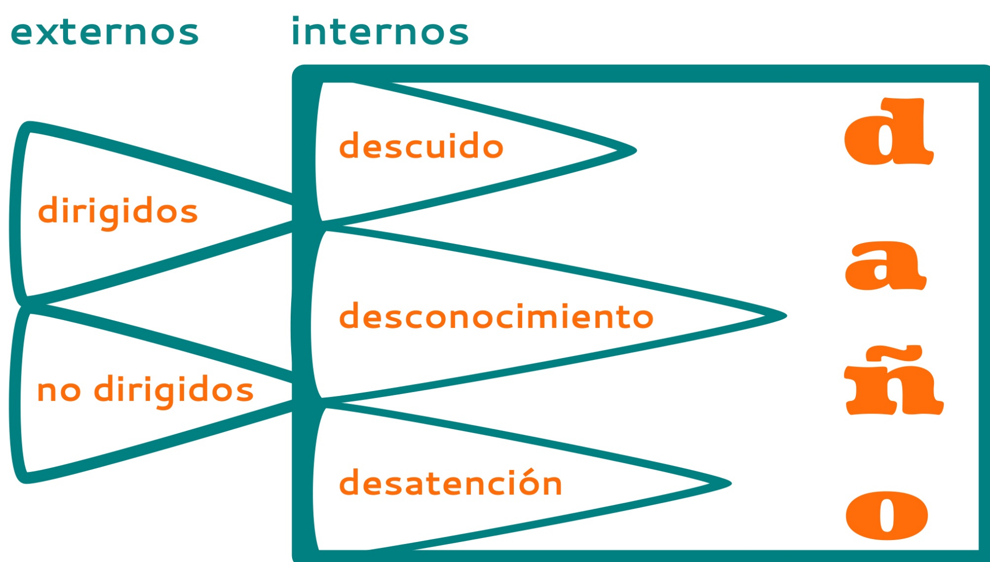
- Es importante mencionar que los IDS no son únicamente aquellos provocados por ataques externos, sino que pueden ser **internos**, producto de un **descuido**, una **desatención** o **desconocimiento** de nuestra parte. En este sentido, el hecho de que un disco externo de nuestra organización sufriera un percance, tras el cual se pierde toda la información en él contenida, es de considerarse un incidente de seguridad digital ya

que si hubiéramos tenido respaldo de la información, ésta no se hubiese perdido. No por tratarse de descuidos internos es menos importante registrarlos. Por el contrario, esta acción nos permite identificar aquellas vulnerabilidades que necesitamos corregir, así como aquellas capacidades que necesitamos potenciar. Una práctica regular de registro y análisis de incidentes de seguridad digital nos permitirá, por ejemplo, darnos cuenta de que en los últimos meses sufrimos un número significativo de incidentes catalogados como "pérdida de información", un llamado de atención para afinar nuestras rutinas de respaldo.

• Entre los **ataques externos** se pueden distinguir aquellos que son **dirigidos**, planificados y ejecutados con el objetivo de hacernos daño y/o obstaculizar nuestro trabajo de defensa, de los **no-dirigidos**, que responden a las amenazas del contexto en el cual nos movemos. En el ámbito digital, ciertas amenazas responden a las políticas de uso de las propias plataformas en las cuales el uso de los datos personales no es optativo, es decir que no es posible elegir si serán o no recolectados o si serán o no compartidos con terceros. En el caso de los ataques dirigidos, algunos son fáciles de distinguir: por ejemplo, la suplantación de identidad en redes sociales, cuando crean un perfil idéntico al nuestro para recabar información y publicar en nuestro nombre, es dirigido, mientras que cuando recibimos un email que ha sido enviado a otras miles de personas para intentar estafar o extraer datos personales (pishing) seguramente no lo sea. Otros en cambio son más insidiosos: las continuas interrupciones a nuestras llamadas telefónicas pueden responder a la escasa calidad de nuestros servicios de telecomunicaciones, así como a intervenciones de llamadas de parte de actores que quieren obtener información. En cualquier caso, el mismo ejercicio regular de registro y análisis de incidentes de ISD nos ayudarán a afinar nuestras capacidades.

• Los ataques externos (dirigidos o no dirigidos) pueden verse potenciados por descuidos, desatenciones o desconocimiento de nuestra parte. Por ejemplo, para el caso de las plataformas de videollamadas comerciales, los datos quedan expuestos a los criterios de privacidad de la empresa dueña de la plataforma. En ese momento **una amenaza de contexto podría elevar el riesgo** si por desconocimiento o descuido en esas llamadas compartimos información sensible o nuestra ubicación.

• En el ámbito digital es importante estimar el costo de un ataque, ya que por ejemplo los malwares dirigidos tienen un costo particularmente elevado, como revela el informe de Artículo 19, R3D y SocialTic, en el cual se estima que el gobierno mexicano gastó entre 15 y 18 millones de dolares en el software de espionaje Pegasus (Artículo 19, R3D, SocialTic; 2017:64).



ESQUEMA 2. CAUSAS DE UN INCIDENTE (EXTERNA, INTERNA Y COMBINACIÓN)

Registrar nuestros Incidentes de Seguridad Digital no significa únicamente tomar nota de ellos, sino entrenarnos para identificarlos y reflexionar acerca de su significado para nuestra labor de defensa de derechos humanos. Desde Sursiendo consideramos el **registro de incidentes de seguridad digital** como una práctica fundamental en dos sentidos: por un lado permite **fortalecer los Cuidados Digitales Colectivos** de nuestros grupos y organizaciones. Por otro, proporciona elementos contundentes para la **investigación-acción, la divulgación** y la **incidencia política** y **pública** en el campo de los derechos digitales.

Los incidentes de seguridad digital son, en efecto, indicadores de la situación particular de seguridad de nuestra organización y colectivo, así como del impacto y trascendencia de nuestro trabajo en derechos humanos mostrándonos, entre otras cosas, qué intereses estamos tocando. A la vez, hablan de la situación de seguridad de quienes defendemos derechos humanos en un determinado contexto, período y área de intervención, y de las prácticas de agresión vigentes en este contexto específico.

Animamos entonces a incluir la práctica de registro de los ISD en las rutinas de nuestras organizaciones y colectivos, así como a poner en común los hallazgos del registro con nuestros aliados para potenciar aquellas iniciativas de denuncia, comunicación y transformación socio-políticas.

¿Para qué identificar, registrar, clasificar y analizar incidentes de Seguridad Digital?	
Como práctica de Cuidados Digitales Colectivos	**Como práctica de investigación-acción, divulgación e incidencia política**
• Para contar con elementos ordenados que nos permitan reaccionar ante un incidente particular. • Para identificar patrones: quiénes sufren los ISD, quiénes son los principales agresores, en qué dispositivo, aplicaciones, o programas suceden, qué tipos de ISD se presentan con mayor frecuencia, en torno a cuáles actividades de defensa de derechos humanos se concentran los ISD.	• Para identificar patrones de agresión, paradigmas y tendencias en determinados contextos, períodos y áreas. • Para identificar las principales vulnerabilidades y capacidades del ámbito digital de organizaciones y colectivos que defienden derechos humanos en determinados contextos, períodos y áreas.

• Para identificar nuestras principales vulnerabilidades y capacidades; corregir las primeras y potenciar las segundas mediante acciones específicas, protocolos, políticas o planes de seguridad.	• Para identificar y visibilizar políticas, leyes y prácticas del campo de las tecnologías digitales que van en detrimento de la privacidad, de la seguridad digital y de los derechos digitales.
• Para contar con elementos ordenados para realizar el análisis de la amenaza a nivel organizativo.	• Para ubicar las necesidades en determinados contextos, períodos y área relacionados con la implementación de software dedicado a la protección digital.
• Para contar con evidencias y pruebas concretas de ataques en nuestra contra que podrían ser utilizadas en instancias de denuncia ya sea pública o jurídica.	• Para identificar vacíos u oportunidades para la incidencia política y pública.
• Para compartir con nuestros aliados los hallazgos de nuestros análisis.	• Para demostrar que la seguridad digital es actualmente un ámbito de riesgo creciente para quienes defendemos derechos humanos.

2.1.- El proceso de Registro de Incidentes de seguridad digital

Desde Sursiendo entendemos el **Registro de ISD** como un proceso que conlleva una serie de acciones:

1.- Identificar los ISD.
2.- Documentar los ISD.
3.- Catalogar los ISD.
4.- Analizar los ISD.

Con el fin de facilitar la práctica de Registro de ISD en Sursiendo hemos elaborado una **herramienta** que está pensada para usarse directamente por grupos, colectivos y organizaciones que defienden derechos humanos. En particular les facilitará las tareas de las etapas: 2. Documentar los ISD; 3. Catalogar los ISD y 4. Analizar los ISD.

La herramienta de registro permite documentar los Incidentes de Seguridad Digital (ISD) de manera ordenada y cronológica para que sea más sencillo identificar los patrones. Si usamos la versión impresa de la herramienta los ISD, se ordenarán en el mismo cuaderno, que debe ser resguardado en un lugar seguro al alcance de todos los integrantes del equipo de nuestra organización o colectivo. En cambio, si preferimos la versión digital de la herramienta se sugiere usar un solo documento que debe estar alojado en un lugar seguro y accesible para todas las personas del equipo, por ejemplo, una nube segura. También deben hacerse respaldos frecuentes de esta información.

La herramienta de Registro de Incidentes de Seguridad Digital que proponemos cuenta con 13 campos:

- Los campos de 1 a 6 permiten documentar el Incidente de Seguridad Digital detectado.
- El campo 7 está pensado para catalogar el Incidente de Seguridad Digital detectado de acuerdo a los “tipos” propuestos por Sursiendo y que se encuentran descritos ampliamente en el Anexo 1 de esta guía.
- Los campos del 8 al 11 permiten realizar un primer nivel de análisis del Incidente de Seguridad Digital detectado.
- Los campos 12 y 13 se refieren estrictamente a la acción del registro.

Para el caso de la versión impresa, en la primera hoja del cuadernillo de registro encontrarán un ejemplo de llenado de la Herramienta de Registro.

La herramienta de registro permite documentar los Incidentes de Seguridad Digital (ISD) de manera ordenada y cronológica para que sea más sencillo identificar los patrones

2.1.1.- Identificar los ISD

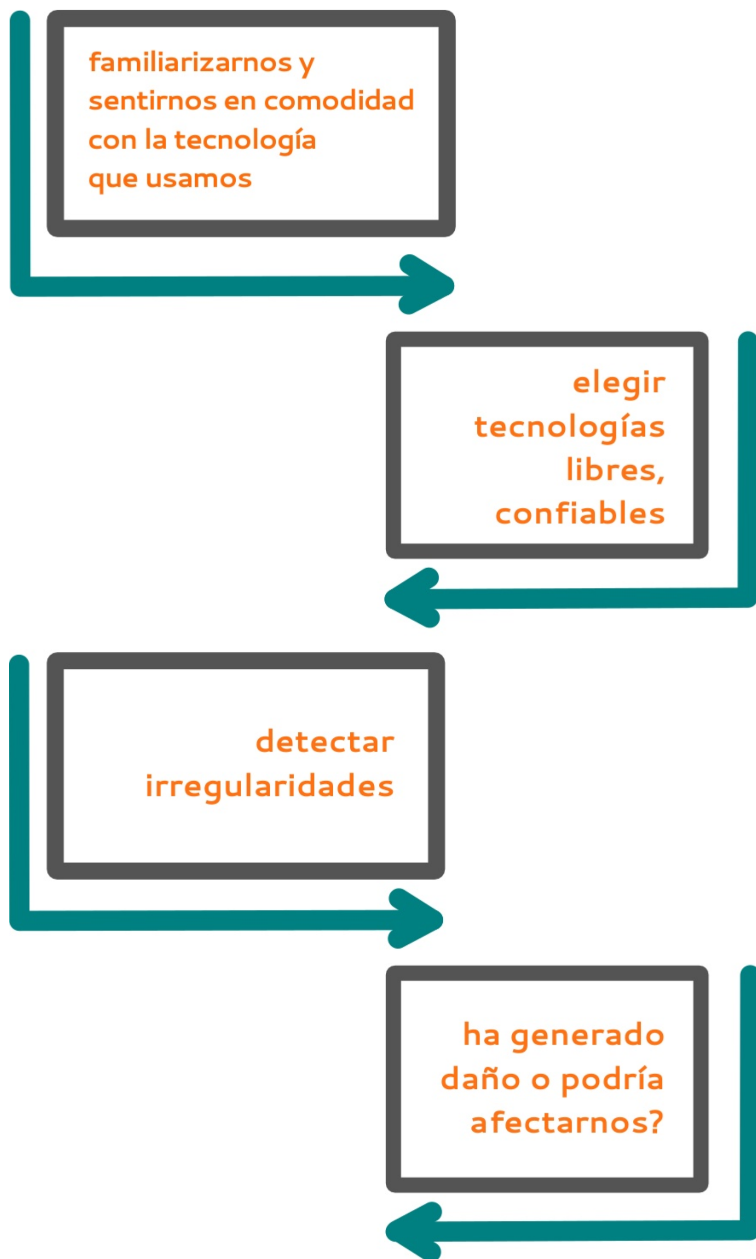
En lo digital la mayoría de incidentes de seguridad suelen manifestarse a través de **irregularidades**, es decir: comportamientos diferentes a lo usual de nuestros dispositivos, aplicaciones, programas o procesos que llevamos a cabo gracias a la tecnología digital, en particular el almacenamiento de la información, la navegación y la comunicación. Es así que

“debemos siempre empezar por el principio y aprender qué señales buscar en nuestros dispositivos y sistemas, que pueden alertarnos acerca de irregularidades” (Tactical Tech; 2016:93).

A diferencia de incidentes que ocurren en el ámbito físico, la mayoría de los ISD son difíciles de identificar, muchas veces no pasan por nuestros cuerpos y normalmente no tenemos “entrenamiento” para detectarlos. Es por eso que necesitamos desarrollar mayores niveles de conciencia acerca de nuestro entorno, que además de permitirnos detectar con rapidez los incidentes, nos ayudará a diferenciar sus niveles de gravedad y así prevenir estados de miedo y paranoia dentro de nuestro colectivo u organización.

Un primer paso de ese entrenamiento es familiarizarnos y sentirnos en comodidad con la tecnología que usamos, hacer el esfuerzo por entender su funcionamiento, elegir programas y aplicaciones que garanticen mayores niveles de control sobre la misma. Tactical Technology Collective denomina tecnologías liberadoras “a aquellas que han sido diseñadas para ser producidas y distribuidas de manera justa, basándose en los principios del software libre y el código abierto, oponiéndose a su 'obsolescencia programada', e incorporando la privacidad y la seguridad en su centro” (Tactical Tech, 2015). No se deben olvidar además aquellas rutinas saludables de mantenimiento y actualización de nuestros equipos, aplicaciones y programas, sin las cuáles aún las mejores tecnologías se tornan en elementos de vulnerabilidad.

Una vez reconocemos cuál es el normal funcionamiento de nuestros dispositivos, utilicemos servicios, aplicaciones y procesos confiables, estaremos listas para detectar sus irregularidades, es decir, los comportamientos raros, extraños o sospechosos, posibles indicios de un ISD. Allí nos tocará preguntarnos si este acontecimiento fuera de lo común ha generado daño o podría afectarnos en términos personales, familiares, comunitarios u organizativos. Si la respuesta es afirmativa hemos detectado un Incidente de Seguridad Digital.



GRÁFICA 3.- DETECCIÓN DE ISD

Esto no quiere decir que todas las irregularidades identificadas resultarán en daños graves, o tendrán impactos negativos en nuestra labor de defensa, sin embargo, es importante registrarlos porque, por un lado, nos guiarán en el desarrollo de nuevas medidas de cuidados internos y por otro, es parte del entrenamiento en la tarea de detección. Poco a poco iremos aprendiendo qué ISD son más significativos que otros, cuáles son fruto de nuestros descuidos, cuáles en cambio dependen del contexto donde trabajamos y cuáles son el producto de ataques como tal. Finalmente en un segundo momento podremos acudir a nuestros compañeros y compañeras y/o a personas y organizaciones de confianza con capacidades técnicas superiores a las nuestras para poder cerciorarnos de nuestras impresiones iniciales.

En la fase de detección, si no tenemos a mano la herramienta de Registro de Incidentes de Seguridad Digital sugerimos tomar notas de la información principal inherente al mismo: fecha, hora, lugar, aplicaciones y usuarios afectados, además de tomar la mayor cantidad de evidencias posibles. Se debe tomar en cuenta que en Internet la información desaparece rápidamente, por lo que es preciso contar con evidencias distintas, que al cruzarse entre sí nos aporten más elementos de análisis. Si detectamos un incidente, por ejemplo un comentario difamatorio en contra de nuestra organización en alguna red social, además de copiar la URL donde éste se ubica, deberíamos realizar una captura de pantalla, para asegurarnos de tener evidencia fehaciente del comentario, que podría ser borrado en cualquier momento. Lo mismo vale para fotografías o vídeos publicados, cuyos metadatos podrían ser modificados o eliminados, y que por ello es importante descargar a tu dispositivo.

Iremos aprendiendo qué ISD son más significativos que otros, cuáles son fruto de nuestros descuidos, cuáles en cambio dependen del contexto donde trabajamos y cuáles son el producto de ataques como tal

2.1.2.- Documentar los ISD

Una vez detectado un ISD lo que sigue es documentarlo, proporcionando la mayor cantidad de información disponible. La documentación además de permitir mantener un registro confiable y ordenado de los ISD que puede ser consultado por nuestro colectivo u organización, facilita las tareas de análisis y reacción ante el ISD.

Para documentar nos apoyamos en la Herramienta de Registro de ISD, en particular en los campos 1 al 6.

Campo 1. Fecha y hora del incidente ¿Cuándo ocurrió el ISD?

Aquí indicaremos la fecha y hora del incidente. Si no las recordamos con precisión nos podemos apoyar en las evidencias recolectadas, ya sea fotografías, capturas de pantalla o notas en papel, o acudir a testigos o personas de confianza que contactamos al momento del incidente. Si fecha y hora de detección son diferentes de cuando sucedió el hecho, se sugiere indicar ambas.

Campo 2. Lugar físico ¿Dónde ocurrió el ISD?

Aquí indicaremos el lugar físico donde aconteció el incidente, el lugar en el cuál nos dimos cuenta del mismo, o, en dado caso, ambos lugares. Aún si se trata de un incidente que aconteció en un "lugar digital", como una página web o una cuenta de correo, es importante dejar constancia de dónde nos encontrábamos al momento de percatarnos del mismo.

Campo 3. Quiénes ¿Quiénes sufrieron el ISD? Nombre de la persona y puesto/cargo en la organización/colectivo.

Si algún integrante de nuestro colectivo u organización es objeto del Incidente de Seguridad Digital detectado hay que señalarlo en ese campo. Lo mismo si se trata de declaraciones de acoso, amenaza, extorsión o difamación en línea que señalan a una o más personas del equipo. En cambio si el incidente involucra una cuenta de correo institucional impersonal o nos encontramos ante una difamación institucional se indicará aquí el nombre de nuestro colectivo u organización. Cuando el incidente involucre también a terceros, es importante señalarlo, indicando además cuál es su vínculo con nuestra organización.

Campo 4. Lugar digital: dispositivos, aplicaciones, páginas web_¿Qué dispositivos, aplicaciones o páginas web fueron afectados por el ISD?

Un ISD suele acontecer en uno de los procesos que realizamos mediante la tecnología, especialmente la navegación, la comunicación o el almacenamiento de información. En este campo proporcionaremos los detalles de los dispositivos, aplicaciones, páginas web, cuentas de correo o de redes sociales donde el ISD se ha manifestado, entre otros, ubicación de las carpetas afectadas en determinado dispositivo, URL de páginas web, dirección de correos, etc.

Campo 5. Relato del ISD. Relata qué aconteció, deteniéndote en todos los detalles que recuerdes.
Este campo está pensado para incluir un relato del ISD y de las circunstancias en que éste fue detectado. Sugerimos relatar el incidente en primera persona y en orden cronológico, incluyendo la mayoría de detalles y aquellas consideraciones subjetivas que ayudarán a enriquecer el análisis.

Campo 6. Evidencias ¿Tenemos evidencias? ¿Dónde están almacenadas? Incluir todas las que se tengan y sean posibles de reunir.
Este campo permite documentar las evidencias que se tienen del incidente con su ubicación. Con evidencias nos referimos a: fotografías, audios, capturas de pantalla, URL y cualquier material que dé cuenta de lo acontecido. En seguridad digital es importante contar con el mayor número de evidencias, y que éstas sean de distintos tipos para que al cruzarlas obtengamos información confiable y "objetiva". Sugerimos almacenar las evidencias de los incidentes de manera ordenada en un lugar seguro, y hacer respaldos regulares de las mismas.

Documentar es una tarea clave del proceso de registro, por ello es importante realizarla lo antes posible después de detectarlo, para evitar que se pierda u olvide información. A la vez se debe procurar que la persona que detectó el incidente sea la misma que lo documente, y que para ello se encuentre en un espacio seguro y haga esa tarea sin prisas. Si la persona que detectó el incidente está alterada, porque le afectó en primera persona o tiene temor de que el incidente tenga consecuencias para su persona, un compañero o compañera podrá encargarse de realizarle las preguntas necesarias para llenar la herramienta.

2.1.3.- Catalogar los ISD

Después de haber documentado el Incidente de Seguridad Digital detectado es importante catalogarlo de acuerdo a "tipos" predeterminados, ya que esta acción potencia nuestras prácticas de Cuidados Digitales Colectivos así como las tareas de investigación y divulgación que de ellos se desprenden, permitiendo:

- Facilitar el análisis haciendo uso de categorías estudiadas por otras personas.
- Dirigir los esfuerzos para potenciar las capacidades internas a nuestro

colectivo/organización y mitigar las vulnerabilidades para prevenir los tipos de ataques más recurrentes y/o dañinos.

- Dirigir los esfuerzos de investigación, ya sea técnica, legal o de seguridad, hacia los tipos de ataques más recurrentes y/o dañinos.
- Reducir la ansiedad gracias al peso específico que cada tipo de ataque puede tener.

Con **tipo de incidente** nos referimos a la manifestación concreta de un ataque dirigido, de una amenaza de contexto o de un descuido humano en nuestros dispositivos y procesos. Cada tipo de ISD se vincula con una serie de daños o afectaciones particulares a nuestra integridad personal, institucional o comunitaria, además de violar derechos humanos específicos.

Para facilitar la tarea de tipificar los IDS, desde Sursiendo hemos elaborado una **Categorización de Incidentes de Seguridad Digital** que pueden encontrar en el Anexo 1 de la presente guía. En él se presentan 19 tipos de incidentes de seguridad digital clasificados según 4 categorías, de acuerdo al proceso afectado por el incidente.

Procesos donde se manifiesta el incidente	Tipos de manifestación
COMUNICACIÓN El ISD se manifiesta en aquellas aplicaciones, programas o servicios que nos permiten llevar a cabo nuestras comunicaciones institucionales: el envío y la recepción de correos electrónicos, en el funcionamiento de nuestras páginas web, blog o cuentas de redes sociales.	1. Recibimos una notificación de intrusión o intento de, a una de nuestras cuentas. 2. Perdimos acceso a nuestra(s) cuenta(s). 3. Estamos teniendo problemas de uso o funcionamiento de correo(s) electrónico(s). 4. Es publicada información personal privada, sin nuestro consentimiento. 5. Es publicada información falsa sobre nuestra persona u organización. 6. Recibimos mensajes de odio, agresivos o mensajes sexuales no solicitados. 7. Recibimos mensajes de amenaza o extorsión. 8. Recibimos un mensaje que solicita realizar una acción con urgencia y/o confirmar información personal. 9. Usurpan nuestra identidad personal u organizativa. 10. Recibimos intrusión en nuestras conversaciones, llamadas y videollamadas.

INFORMACIÓN ALMACENADA El ISD se manifiesta en la información que almacenamos en nuestros dispositivos, en nubes u otras plataformas virtuales.	11. Perdimos información almacenada. 12. Fuimos forzados a entregar o eliminar información o terceras partes pueden ser forzadas a entregar nuestra información. 13. Se realizaron captura de imágenes, audios o videos sin nuestro consentimiento.
NAVEGACIÓN El ISD se manifiesta en aquellas aplicaciones, programas o servicios que nos permiten llevar a cabo la navegación; navegadores y páginas web en particular.	14. Nuestro navegador funciona de manera diferente a lo habitual. 15. Nuestra(s) aplicacion(es), programa(s) o dispositivo(s) funcionan de manera diferente a lo habitual. 16. Nuestra página web está bloqueada o funciona de manera diferente a lo habitual.
HARDWARE El ISD se manifiesta en las partes físicas de nuestros equipos: computadoras, celulares, tablets, red cableada.	17. Daño, pérdida o robo de dispositivo(s). 18. Nuestro(s) dispositivo(s) son inspeccionados sin nuestro consentimiento. 19. Nuestro(s) dispositivo(s) son confiscados por agentes de seguridad. 20. Nuestra red funciona de manera diferente respecto a lo habitual.

* Para la descripción de cada tipo, ir al Anexo 1: Categorización de Incidentes de Seguridad Digital.

En la herramienta de Registro de Incidentes de Seguridad Digital el campo 7 es el destinado a indicar el “tipo” de ISD.

<u>Campo 7. Tipo de ISD. Procesos donde se manifiesta el ISD y tipo de manifestación</u>

Aquí indicaremos el tipo de incidente de acuerdo a la **Categorización de Incidentes de Seguridad Digital** del Anexo. Para detectar el tipo específico nos tendremos que preguntar dónde se manifestó el ISD, y qué procesos fueron afectados.

2.1.4.- Analizar los ISD

El Registro de Incidentes de Seguridad Digital se concluye con un primer momento de análisis a ser desarrollado por quien lo vivió y/o detectó, eventualmente con el apoyo de alguna persona colega, compañera, testigo o técnica de confianza. Ese momento, si bien no debería ser el único destinado al análisis del incidente, permitirá ya valorar algunos impactos, establecer los primeros pasos a seguir, y qué medidas de mitigación emprenderemos.

Para esa tarea fueron pensados los siguientes campos de registro:

Campo 8. Daños: ¿El ISD ha generado algún daño? ¿Se pueden identificar daños certeros de verificarse?
Con daño nos referimos ya sea a afectaciones a personas (físicas o emocionales), perjuicios materiales a nuestros equipos o datos, o al deterioro de nuestra imagen pública. En este campo es importante indicar los daños ya acontecidos y señalar aquellos que consideramos puedan llegar a verificarse, en aras de prevenirlos.

Campo 9. Agresor: ¿Se sabe quiénes están detrás del ISD?
Este campo debe llenarse únicamente cuando se considera que el ISD detectado fue causado por terceros, es decir, que no aplica para aquellos ISD que son consecuencia de nuestros descuidos. En lo digital no siempre es sencillo llegar a identificar al agresor, porque muchas veces los ataques se perpetran a través de malware, botso perfiles no ligados a una identidad real. Sin embargo, les invitamos a hacerse siempre esta pregunta. Muchas veces las intuiciones que tenemos no son fruto de la causalidad sino de nuestro conocimiento de las dinámicas de defensa de derechos humanos, y deben ser tomadas en cuenta en los análisis. Si no se tienen certezas ni pistas suficientes para identificar la identidad de los agresores, se puede dejar ese campo en blanco.

Campo 10. Motivaciones: ¿Por qué crees que ha pasado? ¿Relacionas el ISD con alguna acción de tu organización?
Si ya hemos identificado el agresor podemos rellenar este campo describiendo las que consideramos ser sus motivaciones para provocar el ISD. A la vez, es importante tomar notas de nuestras sospechas acerca

Las intuiciones que tenemos no son fruto de la causalidad sino de nuestro conocimiento de las dinámicas de defensa de derechos humanos, y deben ser tomadas en cuenta en los análisis

de la relación del ISD con alguna actividad de defensa de derechos humanos que hemos realizado, estamos planificando o realizaremos. Tal y como mencionábamos en el campo anterior, no tengamos temor de anotar aquí argumentaciones no comprobadas, ya que nuestras intuiciones pueden dar pistas importantes y todo será analizado en un segundo momento.

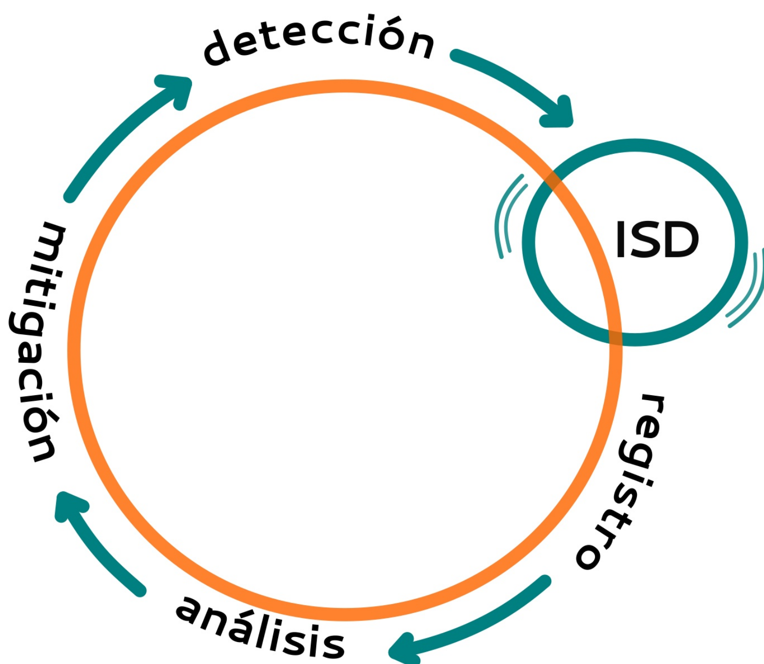
Campo 11. Seguimiento: ¿Qué acciones fueron tomadas para reaccionar al ISD?

Si ya tomamos o planificamos acciones específicas para reaccionar ante el ISD detectado, éste es el campo para documentarlas. Sería importante asociar a cada acción el resultado que se espera lograr en términos de mitigación del daño. Si aún no se tienen acciones planificadas este campo puede llenarse en un segundo momento.

Para dar seguimiento al Registro de Incidentes, asegurarse que cada incidente sea registrado, debidamente analizado y que se tengan medidas de respuesta, es importante designar una persona responsable de la Herramienta de Registro. Si su organización cuenta con una persona encargada de la Seguridad (ya sea integral o digital) podría ser la indicada para ese rol; en su ausencia pueden decidir que se trate de una responsabilidad rotativa, para fomentar la corresponsabilidad.

Finalmente, es importante cuidar la Herramienta de Registro, ya que contiene información muy sensible de nuestro colectivo u organización, de las personas que la conformamos, así como de nuestros familiares, aliados y personas cercanas. Compartiremos la información contenida en la Herramienta únicamente con personas y organizaciones de confianza, que de algún modo están implicadas en uno o más Incidentes, que podrían ser afectados por ellos o que nos puedan ayudar en el análisis.

El proceso de Registro de Incidentes de Seguridad Digital debe verse como un ciclo que empieza con la detección y termina con el análisis que es en sí mismo un proceso de aprendizaje. A más incidentes documentados, catalogados y analizados más capacidades habremos adquirido para la detección de los incidentes que acontecerán en el futuro. No debe olvidarse además que no se trata de un proceso aislado, que su propósito no termina aquí sino que debe enlazarse con el análisis de riesgo y amenaza que describimos en el capítulo 1.



ESQUEMA 4. CICLO DE ISD

Conclusiones

Cierres y vueltas

"Al principio no entendía claramente la importancia de la seguridad digital, pero cuando empezamos a analizar sobre nuestra manera de trabajar, y cómo desarrollamos todas nuestras actividades, entendí los riesgos a los que somos vulnerables" (Integrante de una organización social de Chiapas, 2020)

Hemos llegado al final de nuestro recorrido en el que aprendimos cómo realizar el Registro de nuestros Incidentes de Seguridad Digital (ISD), a identificarlos, documentarlos, catalogarlos y realizar un primer nivel de análisis. Si bien no entra en los propósitos de la presente Guía ofrecer una metodología detallada para analizar a profundidad los Incidentes de Seguridad Digital, queremos concluir con algunas recomendaciones generales sobre cómo emprender un análisis de ISD de manera autónoma, eficaz y colectiva.

- Cada ISD merece ser compartido con todas las personas que conforman su colectivo/organización, además de terceras personas que podrían resultar perjudicadas por el mismo. La socialización de los ISD requiere de un espacio seguro.

- Cada ISD debe ser analizado con detenimiento por al menos dos personas de nuestras organizaciones y colectivos, con el objetivo de proponer acciones de respuesta y mitigación específicas y adecuadas a ser discutidas con el resto del equipo.

- Las preguntas básicas para guiar el análisis de ISD son las mismas que propusimos en la herramienta de Registro: ¿Qué fue lo qué pasó? ¿Cómo nos afectó o puede afectar el ISD? ¿Quiénes son los perpetradores? ¿Cuáles son sus motivaciones y a cuáles acciones de defensa de

El objetivo de los análisis más integrales es relacionar los incidentes entre sí, y a través de esta acción concreta evaluar el nivel de amenaza que estamos enfrentando

derechos humanos las relacionamos? ¿Qué acciones podemos emprender para mitigar los daños ya hechos, o para prevenir aquellos que pueden depender del incidente? ¿Qué acciones podemos emprender para fortalecernos a lo interno de nuestro colectivo y así evitar que pasen incidentes de ese tipo en el futuro? ¿Cómo podemos cuidar a las personas afectadas por el incidente en su integralidad?

- En el diseño de las acciones de reacción a los ISD hay que buscar prevenir afectaciones y daños a nuestra organización: a nivel personal, colectivo, de nuestros dispositivos, aplicaciones, información e imagen pública. Asimismo es importante asegurarnos que las acciones prevengan futuros incidentes o, al menos, que nos permitan enfrentarlos con más preparación. Acciones de reacción puede haber de muchos tipos: técnicas, de denuncia legal o pública, de incidencia política, de comunicación, búsqueda de asesoría técnica, legal o administrativa, fondos específicos destinados a la compra de equipo, al análisis forense, a la seguridad de nuestras oficinas.

- Además de analizar el ISD en su singularidad, es importante llevar a cabo análisis regulares que tomen en cuenta al mismo tiempo Incidentes de Seguridad Física y de Seguridad Digital sucedidos en determinado período de tiempo. Estos análisis requieren de la participación de todas las personas que conforman nuestros equipos. Para estos momentos es bueno prever una facilitación (ya sea interna o externa) y una relatoría. El objetivo de los análisis más integrales es relacionar los incidentes entre sí, y a través de esta acción concreta evaluar el nivel de amenaza que estamos enfrentando. Después será posible diseñar medidas pertinentes para elevar nuestras capacidades y disminuir nuestras vulnerabilidades internas.

- Los análisis regulares de varios incidentes a la vez pueden empezar con la realización de una línea de tiempo en la que se colocan de manera cronológica los incidentes físicos y digitales. Cada incidente será detallado mediante la información ya contenida en la sección de documentación de la Herramienta de Registro: ¿dónde y cuándo pasó? ¿Quiénes fueron los afectados? ¿De qué tipos de incidente se trata?, etc.

- En el análisis es importante encontrar patrones de las agresiones dirigidas, así como de aquellos descuidos internos o amenazas de contexto. En particular, nos debemos fijar en qué tipos de incidentes son más recurrentes, cuáles producen daños más serios o afectan más el desarrollo de nuestras acciones de defensa de los derechos humanos.

- Al final del análisis habremos establecido qué nivel de amenaza estamos enfrentando, cuáles son sus impactos presentes, y cuáles podrían ser los impactos a futuro. Habremos identificado los principales actores que se oponen a nuestro trabajo, así como caracterizado sus prácticas de agresión.

- Las medidas a implementar que se desprenden de estos análisis pueden ser de múltiple naturaleza. Los más comunes abarcan: la elaboración, actualización o corrección de Protocolos o Planes de Seguridad Integral o Digital específicos, ajustar rutinas cotidianas de trabajo, inscripción a cursos u otros procesos de fortalecimiento sobre temas específicos, campañas de sensibilización o denuncia de agresiones específicas, construcción de redes de protección con actores aliados.

Después del análisis de uno o más ISD que nos afectaron, puede ocurrir que necesitemos el apoyo de una persona experta en tecnología. Ya sea porque no entendemos exactamente qué fue lo que pasó, porque no logramos identificar las medidas adecuadas para fortalecer nuestra seguridad o diseñar acciones técnicas específicas para llevar a cabo y prevenir futuros incidentes. Desafortunadamente hay situaciones y contextos donde no existen organizaciones locales que se dedican a la Seguridad Digital y/o encontrar un Soporte Técnico de confianza no es tarea sencilla. También puede suceder que no tenemos fondos destinados para esos pagos o simplemente no les tenemos suficientes confianza.

Para responder a estas situaciones a lo largo de América Latina en los últimos años surgieron iniciativas que pueden apoyarnos en diversos sentidos, constituyendo un “ecosistema de apoyo de seguridad digital, un ecosistema en expansión compuesto por organizaciones, individuos, colectivos y grupos de múltiples partes interesadas que buscan brindar apoyo de seguridad a la sociedad civil” (The Engine Room, 2018:4).



Si requieren apoyo con el análisis o la reacción ante un Incidente de Seguridad Digital les recomendamos contactar:

- al Observatorio Centroamericano de Seguridad Digital, de Fundación Acceso, si se encuentran en Guatemala, Honduras, El Salvador y Nicaragua. Su correo de contacto es: observatoriosd@acceso.or.cr

- a la Línea de Ayuda en Seguridad Digital, de Access Now, a través de su formato de contacto, que encuentran en la página: www.accessnow.org/help-es/

- al Contacto de Emergencia, de Front Line Defenders, a través del correo: americas@frontlinedefenders.org

- a Digital Defenders Partnership, de Hivos, a través del correo: team@digitaldefenders.org

Estas iniciativas brindan apoyo gratuito y en español sobre diversos servicios, como la asistencia técnica, el asesoramiento directo en tiempo real y la evaluación de los riesgos a personas y organizaciones que defienden derechos humanos y están enfrentando algún tipo de amenaza digital. Además, están en contacto con organizaciones locales que pudieran ser recomendadas para procesos más cercanos. Finalmente, también pueden escribirnos a ***sursiendo [arroba] sursiendo.org.*** Si bien no contamos con un servicio de *Help Line* podemos hacer de puente con otras organizaciones y grupos que proporcionan ese tipo de apoyos.

Como vimos en los capítulos anteriores, el Registro de Incidentes de Seguridad Digital es una tarea chiquita pero importante, ya que abona a los Cuidados Colectivos de nuestras organizaciones y grupos, y a la expansión del espacio para la defensa de los derechos humanos, más allá de lo digital. Como en otras prácticas de protección cuánto más energías colectivas le dediquemos, mayores y más rápidos serán los resultados. Haciendo es como se aprende.

Les invitamos entonces a lanzarse a esta tarea, y al cabo de un período de tiempo elegido desde el inicio, sentarse a reflexionar con todas las personas que conforman sus colectivos y organizaciones, acerca de cómo les ha ido, identificar qué acciones funcionaron mejor y cuáles en cambio requieren ser revisadas. Desde Sursiendo nos interesa mucho conversar acerca de su experiencia con el Registro, sus hallazgos, sus dudas o problemas, porque el conocimiento se construye y perfecciona a través del diálogo colectivo.

Como en otras prácticas de protección cuánto más energías colectivas le dediquemos, mayores y más rápidos serán los resultados. Haciendo es como se aprende

Anexo

Categorización de Incidentes de Seguridad Digital

Tipo	Descripción e indicaciones para su identificación	Ámbitos donde se manifiesta el incidente
1. Recibimos una notificación de intrusión o intento de, a una de nuestras cuentas.	Se refiere a cuando recibimos una notificación de parte de nuestros proveedores de correo electrónico, redes sociales u otros servicios, informándonos acerca de un intento fallido de acceso a nuestras cuentas, del acceso exitoso a una de nuestras cuentas desde dispositivos que no reconocemos o una notificación solicitándonos ingresar nuestras credenciales de cuenta. Si no reconocemos estas acciones podríamos estar siendo objeto de un **intento de intrusión de cuenta,** de un **ataque de phishing** o de una **infección por malware**. También es posible que se trate de una acción directa de nuestra parte como ingresar a las cuentas desde un dispositivo diferente al habitual. La intrusión de cuentas es una práctica de agresión que puede ser dirigida en contra de quienes defienden derechos humanos para tomar el control de sus cuentas, acceder a su información, y causar daño de diversa índole. El ingreso no autorizado a una cuenta implica posibles actos de **usurpación de identidad, extorsión, intimidación, amenaza, acoso o difamación.** La intrusión de cuenta viola nuestros derechos a la **privacidad**, a la **libertad de expresión** y **asociación** y el **derecho a defender derechos humanos**, puesto que almacenamos en nuestras cuentas de correo y redes sociales información privada e información inherente a violaciones de derechos humanos y, en muchas ocasiones, son medios que nos permiten llevar a cabo actividades propias de nuestra labor, como la comunicación.	COMUNICACIÓN

2. Perdimos acceso a nuestra(s) cuenta(s)	Se refiere a cuando al utilizar nuestros datos para ingresar a una de las cuentas personales o institucionales, el acceso nos es negado. Una posibilidad es que nuestras cuentas hayan sido denunciadas y/o dadas de baja. También podríamos haber sido objeto de un **ataque de phishing** o de una **infección por malware dirigidos o no dirigidos,** en algunos casos acompañado de un mensaje de extorsión. Finalmente, es posible que se trate de otro tipo de **descuido o desconocimiento** como el hecho de que intentamos acceder a una cuenta desde diferentes dispositivos a la vez, nuestras contraseñas sean demasiado sencilla y fueron vulneradas, usamos la misma contraseña para diversas cuentas, hemos olvidado la contraseña y eso es aprovechado para bloquear nuestras cuentas y/o para realizar una intrusión. Bloquear el acceso a las cuentas de quienes defienden derechos humanos de manera intencionada es una práctica de agresión que busca limitar nuestro espacio de actuación y causar daño. Si constatamos que el ataque proviene del Estado se podría tratar de **censura en línea**. Bloquear nuestras cuentas personales o institucionales viola nuestros derechos a la **privacidad, a la libertad de expresión y asociación y el derecho a defender derechos humanos**, puesto que almacenamos en nuestras cuentas de correo y redes sociales información privada e información inherente a violaciones de derechos humanos, y, en muchas ocasiones, son medios que nos permiten llevar a cabo actividades propias de nuestra labor, como la comunicación.	COMUNICACIÓN
3. Estamos teniendo problemas de uso o funcionamiento con correo(s) electrónico(s).	Se refiere a cuando alguno de nuestros correos electrónicos, ya sean personales o institucionales, funciona de manera distinta a la habitual. Podríamos haber sufrido una intrusión por parte de terceros, existir un problema con nuestro servidor o podríamos haber sido objeto de un ataque de malware. También es posible que se trate de un descuido o desconocimiento como el haber realizado	COMUNICACIÓN

	una configuración incorrecta de nuestro correo. Finalmente la política de proveedores de correo comerciales nos expone a amenazas de contexto como la invasión de nuestra privacidad por publicidad dirigida. Algunas de las señales de funcionamiento incorrecto del correo electrónico son: • uno o más correos electrónicos enviados no llegan a la persona destinataria, • la información de mi correo electrónico es interceptada, • se marcan como leídos mensajes que no he leído, recibo correos de destinatarios desconocidos que contienen información confidencial, • recibo correos inusuales de destinatarios conocidos. En caso de ataque dirigido se estarían violando nuestros derechos a la **privacidad, a la libertad de expresión y asociación y el derecho a defender derechos humanos**, puesto que almacenamos en nuestras cuentas de correo y redes sociales información privada e información inherente a violaciones de derechos humanos, y, en muchas ocasiones, son medios que nos permiten llevar a cabo actividades propias de nuestra labor, como la comunicación.	
4. Es publicada información personal privada, sin nuestro consentimiento	Se refiere a cuando se publica información acerca de nuestra persona u organización, ya sean fotos, vídeos, descripción personal, ubicación, etc. sin nuestro consentimiento. La política de proveedores de redes sociales comerciales nos expone a amnazas de contexto como la invasión de nuestra privacidad o la compartición de información personal sin nuestro consentimiento. Por otra parte, podríamos estar siendo objeto de **doxxing, ciberpatrullaje, usurpación de identidad, o acoso en línea.** Por **descuido o desconocimiento** publicamos a menudo información personal en redes sociales y otros espacios de acceso público y ésta puede ser usada en nuestra contra. Publicar información privada sin consentimiento es una práctica de agresión que podría poner en riesgo la vida y el trabajo de quienes defendemos derechos humanos, puede desacreditar nuestra labor y cerrar nuestros espacios de actuación. Además una vez un contenido privado es difundido, se pueden mantener copias del mismo en distintos	COMUNICACIÓN

	dispositivos, aplicaciones, páginas web y nubes y no tendremos control sobre la distribución de los mismos. En este caso se trata de una violación a nuestro **derecho a la privacidad** puesto que cada persona defensora debe poder decidir qué información quiere compartir, con quiénes y de qué formas.	
5. Es publicada información falsa sobre nuestra persona u organización.	Se refiere a cuando se publica información falsa acerca de nuestra persona u organización en redes sociales, páginas web u otras plataformas digitales. Podríamos estar siendo objeto de **difamación**. Ésta es una práctica de agresión con frecuencia usada en contra de quienes defienden derechos humanos, con el objetivo de provocar daño, desacreditar nuestro trabajo, limitar nuestro espacio de actuación, instigar a la violencia y justificar la criminalización en nuestra contra. La difamación viola nuestro **derecho a la privacidad, a la integridad personal, y a defender derechos humanos** puesto que expone nuestra información privada, causa daño a nuestra esfera emocional y a nuestra imagen pública, componente importante de nuestra labor.	COMUNICACIÓN
6. Recibimos mensajes de odio, agresivos, intimidatorios o mensajes sexuales no solicitados.	Se refiere a cuando recibimos mensajes de odio, mensajes agresivos o intimidatorios, contenidos sexuales no solicitados por correo electrónico, en redes sociales, u otro medio digital. Podríamos estar siendo objeto de **doxxing, acoso en línea y/o intimidación en línea.** Todos las anteriores son prácticas de agresión a menudo dirigidas en contra de quienes defienden derechos humanos con el objetivo de causar daño, limitar nuestros espacios de actuación, e instigar violencia en nuestra contra. En particular el acoso en línea es un tipo de violencia de género que es usado en contra de mujeres defensoras y personas de la comunidad LGTBIQ+. En el ámbito digital ese tipo de ataques puede ser realizado por **trolls, bots o perfiles específicamente creados para estos fines** que complican identificar a la persona agresora.	COMUNICACIÓN

	Este tipo de mensaje viola nuestro derecho a la integridad personal, a la libertad de expresión y a defender derechos humanos puesto que causa daño a nuestra esfera emocional, afecta nuestra imagen pública y/o nuestras actividades de comunicación, componentes importantes de nuestra labor.	
7. Recibimos mensajes de amenaza o extorsión.	La amenaza y la extorsión son declaraciones que pretenden forzarnos a realizar alguna acción a través de la promesa de un daño o un castigo en nuestra contra. La extorsión en particular tiene la finalidad de conseguir dinero. Se trata de prácticas de agresión a menudo perpetradas en contra de quienes defienden derechos humanos con el objetivo de hacernos daño, interrumpir nuestro trabajo o forzarnos a realizar una acción que de otro modo no haríamos. En el ámbito digital muchas veces son llevados a cabo mediante **bots, trolls, o perfiles específicamente creados para estos fines** que complican identificar a la persona agresora. También es posible que estas agresiones sean el resultado de una infección por ***malware***, en particular los llamados *ransomware, spyware, keylogger* o similares. Si recibimos mensajes de amenaza o extorsión estamos sufriendo una violación a nuestros derechos a la **integridad personal y a defender derechos humanos** puesto que éstos causan daño a nuestra esfera emocional, afecta nuestra imagen pública y/o nuestras actividades de comunicación, componentes importantes de nuestra labor.	COMUNICACIÓN
8. Recibimos un mensaje que solicita realizar una acción con urgencia y/o confirmar información personal.	Se refiere a cuando recibimos un mensaje, notificación o correo electrónico en el cual se nos pide ingresar información personal, como usuarios o contraseñas, o se nos solicita acceder a un link o descargar un archivo de manera "urgente". Podríamos estar siendo objeto de un **ataque de phishing y/o de suplantación de identidad.** Puede ser ataques dirigidos o generalizados. Ese tipo de práctica de agresión se realiza desde correos electrónico o contactos que parecen reales y páginas web que parecen confiables pero también desde correos electrónicos desconocidos.	COMUNICACIÓN

	El objetivo es engañarnos y/o extorsionarnos para instalar un ***malware*** en nuestros dispositivos, o tener acceso a nuestros datos personales como contraseñas o información financiera. El ataque de phishing viola nuestros derechos a la **privacidad, y a defender derechos humanos** puesto que expone nuestra información privada y/o inherente a violaciones de derechos humanos que almacenamos para nuestra labor.	
9. Usurpan nuestra identidad personal u organizativa.	Se refiere a cuando se crean perfiles o correos electrónicos con nuestro nombre y/o de nuestras organizaciones o clonan nuestros sitios web. Podríamos estar siendo objeto de **usurpación de identidad.** Puede ser usada para llevar a cabo actos de **acoso en línea, difamación, extorsión, intimidación o amenaza** en contra de quienes defienden derechos humanos, y resulta particularmente eficaz para desacreditarnos a nivel personal y profesional. La usurpación de identidad viola nuestros derechos a la **integridad personal, a la privacidad, a la libertad de expresión, y a defender derechos humanos** puesto que causa daño a nuestra esfera personal, expone nuestra información privada, afecta nuestra imagen pública y/o nuestras actividades de comunicación, componentes importantes de nuestra labor.	COMUNICACIÓN
10. Recibimos intrusión en nuestras conversaciones, llamadas y videollamadas.	Se refiere a cuando nuestras llamadas, conversaciones o vídeo conferencias son interrumpidas por personas no invitadas. Podríamos estar siendo objeto de **intrusión de nuestras comunicaciones.** Ésta es una práctica de agresión emprendida en contra de defensores de derechos humanos con el fin de obtener información a partir de nuestras comunicaciones, intimidarnos y/o provocar daño. Se puede acompañar de actos de **amenaza, extorsión u acoso en línea**, y puede ser fruto de una acción anterior de doxxing. La intrusión de las comunicaciones es un ataque dirigido que puede **verse facilitado por descuidos, desatenciones o desconocimiento** de nuestra parte como realizar llamadas por medio de aplicaciones no seguras.	COMUNICACIÓN

	La intrusión de las comunicaciones viola nuestros derechos a la **privacidad, a la libertad de expresión y de asociación**, puesto que expone nuestra información privada, afecta nuestra imagen pública y/o nuestras actividades de comunicación, componentes importantes de nuestra labor.	
11. Perdimos información almacenada.	Se refiere a cuando perdemos documentos, fotos, vídeos, u otro tipo de información almacenada en nuestros dispositivos. Podríamos estar siendo objeto de **infección por malware**, de un **daño provocado al hardware**, así como haber incurrido en algún **descuido o desconocimiento**. La falta de rutinas de mantenimiento de dispositivos, los cortes o cambios de tensión en la electricidad y la obsolescencia del hardware pueden causar que nuestros dispositivos no funcionen correctamente y que la información en ellos almacenada se pierda. Rutinas regulares de respaldo de la información podrían evitarnos este incómodo incidente. Además, es común usar nuestros correos electrónicos para almacenar información. Eso nos expone a las políticas particulares de los servidores de correos que podrían derivar en pérdida de esa información. En caso de un ataque dirigido, por ejemplo a través de un malware, nuestra información podría no solo perderse, sino quedar expuesta, lo que podría provocarnos otro daño a futuro. En caso de ataques dirigidos se estarían violando nuestros derechos a la **privacidad, a la libertad de expresión y el derecho a defender derechos humanos**, puesto que expone nuestra información privada y de terceros y/o información sobre violaciones a derechos humanos que recabamos para nuestra labor.	INFORMACIÓN ALMACENADA
12. Fuimos forzados a entregar o eliminar información o terceras partes pueden ser forzadas a entregar nuestra información.	Se refiere a cuando autoridades estatales, crimen organizado u otros actores que pretenden restringir nuestra labor de defensoría nos fuerzan a entregar y/o eliminar información almacenada en nuestros dispositivos, de la que podemos o no tener respaldo. Ésta puede quedar expuesta y/o perdida para siempre.	INFORMACIÓN ALMACENADA

	También puede ocurrir que autoridades soliciten a nuestros proveedores de correos, redes sociales u otros servicios, la entrega de nuestra información por medio de un requerimiento legal, sin que recibamos un aviso. Una vez información privada es expuesta, copias de la misma podrían ser alojadas en distintos dispositivos, aplicaciones, páginas web y nubes y no tendremos conocimiento acerca de la distribución de la misma, lo que podría implicar daños futuros tanto para nuestra persona, nuestro trabajo como las personas con quienes trabajamos. La entrega forzada de información es una violación a nuestros derechos a la **privacidad, a la libertad de expresión y a defender derechos humanos**, puesto que expone nuestra información privada y de terceros y/o información sobre violaciones a derechos humanos que recabamos para nuestra labor.	
13. Se realizaron captura de imágenes, audios o videos sin nuestro consentimiento.	Se refiere a cuando se capturan fotos, grabaciones de audio o vídeos de nuestra persona o nuestras actividades sin consentimiento. Podríamos estar siendo objeto de **vigilancia y/o intimidación**. Éstas son **prácticas de agresión** a menudo usadas en contra de quienes defienden derechos humanos, que pueden ser llevadas a cabo por autoridades estatales, personas particulares y/o dispositivos externos como drones, cámaras de vigilancia o malware que se instala en nuestros dispositivos activando cámaras y micrófonos. Las imágenes y los audios capturados, podrían ser usados para perpetrar actos de **amenazas, difamaciones o extorsiones.** Lo anterior viola nuestros derechos a la **privacidad, a la libertad de expresión y asociación y el derecho a defender derechos humanos** puesto que expone nuestra información privada y la de terceros obstaculizando actividades ligadas a nuestra labor.	INFORMACIÓN ALMACENADA
14. Nuestro navegador funciona de manera diferente a lo habitual.	Se refiere a cuando nuestro navegador funciona de manera diferente a lo usual. Podríamos estar siendo objeto de una **infección por malware dirigido o no dirigido** o haber incurrido en un d**escuido o desconocimiento**, como usar un navegador inseguro, carecer de rutinas de mantenimiento del sistema.	NAVEGACIÓN

	operativo o no haber instalado complementos que mejoran la seguridad de nuestro navegador. Algunas de las señales de funcionamiento incorrecto del navegador son: • el motor de búsqueda predeterminado fue sustituido por otro que no elegimos, • aparecen extensiones o complementos desconocidos, • la página de inicio es diferente a la que elegimos, existen nuevas herramientas en la barra de herramientas, • el buscador arroja resultados inusuales, no acordes con lo solicitado o con lo que habitualmente responde a un tipo de búsqueda específico. En caso de ataque dirigido se trata de una violación a nuestros derechos a la **privacidad, a la libertad de expresión, y a defender derechos humanos**, puesto que expone nuestra información privada y de terceros y/o información sobre violaciones a derechos humanos que recabamos para nuestra labor, y afecta nuestras actividades de comunicación, componente clave de la labor de defensa.	
15. Nuestra(s) aplicacion(es), programa(s) o dispositivo(s) funcionan de manera diferente a lo habitual.	Se refiere a cuando nuestras aplicaciones, programas o dispositivos (celular, computadora, disco externo, usb, etc) funcionan de manera diferente a como lo hacen habitualmente. Podríamos estar siendo objeto de una infección por malware dirigido o no dirigido o haber incurrido en descuido o desconocimiento como la falta de rutinas de mantenimiento de nuestro sistema operativo. Algunas de las señales del funcionamiento incorrecto de aplicaciones y programas son: • el dispositivo está muy lento y/o las aplicaciones fallan especialmente tras iniciarlo, • el dispositivo se reinicia frecuentemente por sí solo, • el dispositivo se calienta y/o los ventiladores funcionan de manera acelerada, • la luz indicadora de actividad de la cámara web está encendida mientras la cámara web no está en uso, • la batería se descarga muy rápido o falla repentinamente, • el cursor realiza movimientos erráticos, • el sistema operativo falla de pronto, se detiene y/o aparece una pantalla azul con un código de error.	NAVEGACIÓN

	• las actualizaciones del sistema operativo y/o los parches de seguridad producen fallos, • no abre alguna aplicación o programa o se abre con irregularidades (no se ve bien, no guarda lo archivos como debería o se modifican los campos del programa como barras de herramientas, etc), • las ventanas se muestran con intermitencias, aún tras comprobar que nuestro monitor funciona correctamente, • aparecen advertencias de antivirus al descargar un archivo y/o ejecutarlo o al conectar un dispositivo extraíble como memorias, usb, discos duros externos o dispositivos móviles (celulares, tablets, ipods, etc), • sospechamos de una intervención telefónica: reconocemos que son una práctica de agresión extendida desde antes de la era digital y sin embargo resulta muy compleja su detección ya que no se pueden prever y requieren de un análisis integral para poder confirmarlas. En caso de una infección dirigida, se estarían violando nuestros derechos a la **privacidad, a la libertad de expresión y asociación**, además de nuestro **derecho a defender derechos humanos** puesto que nuestras aplicaciones, programas y dispositivos permiten llevar a cabo distintas actividades esenciales en nuestra labor de defensa, como el almacenamiento y procesamiento de la información y la comunicación, componentes clave de nuestra labor de defensa.	
16. Nuestra página web está bloqueada o funciona de manera diferente respecto a lo habitual	Se refiere a cuando nuestra web institucional presenta un funcionamiento diferente a lo habitual. Podríamos estar siendo objeto de una **infección por malware dirigido o no dirigido**, un **ataque de denegación de servicio (DDoS)**, **censura en línea, usurpación de identidad,** o haber incurrido en **descuido o desconocimiento**: falta de actualización de nuestra página, instalación de plugins no verificados o desactualizados, falta de pago de servicios de internet, inconvenientes debido a la falta de mantenimiento, entre otros. Algunas de las señales del funcionamiento incorrecto de nuestras páginas son: • no se puede acceder a la dirección web de nuestra página	NAVEGACIÓN

	• aparecen contenidos que no hemos publicado, • no es posible crear nuevos contenidos, • están siendo bloqueados los comentarios. En caso de un ataque dirigido, ya sea por malware o censura, se estarían violando nuestros **derechos a la libertad de expresión y asociación y el derecho a defender derechos humanos** puesto que nuestra página web nos permite realizar actividades de comunicación y vinculación, posicionar nuestras voces y ampliar nuestro espacio de actuación, componentes clave de nuestra labor de defensa.	
17. Daño, pérdida o robo de dispositivo(s)	Computadoras y teléfonos celulares son objetivos fáciles para la delincuencia común, pero también podemos sufrir robos dirigidos por parte de actores interesados en nuestra información. El extravío de los dispositivos también puede ser producto de nuestros **descuidos**, situaciones de tensión psicológica y/o estrés. Si uno de nuestros dispositivos se daña, se pierde, o es robado, la información en él contenida estará expuesta y, en el caso de no haber sido previamente respaldada, perdida. En caso de robo dirigido además nuestra información personal y laboral podría caer en mano de actores que se oponen a nuestro trabajo y abrir el paso a prácticas de **agresión** como la **intimidación, la amenaza, la extorsión, el acoso, o la difamación.** En muchas situaciones es difícil distinguir un extravío causado por descuido humano de un robo así como un robo por delincuencia común de un robo dirigido, por ello es importante realizar un análisis caso por caso. En caso de un robo ya sea o no dirigido, se estarían violando nuestros derechos a la **integridad personal, a la privacidad, a la libertad de expresión y asociación y a defender derechos humanos** puesto que nuestros dispositivos son instrumentos que permiten llevar a cabo distintas actividades esenciales en nuestra labor de defensa, como la comunicación, recabar y almacenar información.	HARDWARE

18. Nuestro(s) dispositivo(s) son inspeccionados sin nuestro consentimiento.	Se refiere a cuando teléfonos, computadoras, usbs, cámaras, servidores u otros dispositivos son **inspeccionados** sin nuestro consentimiento. Puede suceder que en espacios públicos o privados como en nuestros domicilios u oficinas personas cercanas o agentes del Estado ingresen en nuestros dispositivos accediendo a cuentas y/o información allí almacenada. La inspección de nuestros dispositivos es un ataque dirigido que puede **verse potenciado por descuidos, desatenciones o desconocimiento** de nuestra parte como la falta de contraseñas fuertes o tener dispositivos sin encriptar. También puede ser **producto de coacción** por parte de agentes de Seguridad del Estado o responder a un tipo de violencia de género usado en contra de mujeres defensoras y personas de la comunidad LGTBIQ+. La revisión de nuestros dispositivos sin nuestro consentimiento viola nuestros derechos a la privacidad, a la libertad de expresión y asociación, además del derecho a defender derechos humanos puesto que nuestros dispositivos son instrumentos que permiten llevar a cabo distintas actividades esenciales en nuestra labor de defensa, como la comunicación, recabar y almacenar información.	HARDWARE
19. Nuestro(s) dispositivo(s) son confiscados por agentes de seguridad.	Se refiere a cuando agentes de seguridad del Estado solicitan **confiscar** nuestros teléfonos, computadoras, usbs, cámaras, servidores u otros dispositivos en un allanamiento a nuestras oficinas o casas, retén, cruce fronterizo, puesto de control de seguridad, con el objetivo de analizar su contenido. Si la inspección es generalmente una operación de corto plazo, la confiscación podría llegar a tomar más tiempo sin que se nos avise cuánto duraría. En ambos casos la información contenida en nuestros dispositivos está irremediablemente expuesta, y nuestros dispositivos vulnerables a **infección por malware o instalación de otro tipo de *software* o *harware*** específico para el registro de pulsaciones (como *keylogger*). La confiscación de dispositivos sin una orden judicial violan nuestros derechos a la **privacidad, a la libertad de expresión y asociación, además del derecho a defender derechos humanos** puesto que nuestros	

	dispositivos son instrumentos que permiten llevar a cabo distintas actividades esenciales en nuestra labor de defensa, como la comunicación, recabar y almacenar información.	
20. Nuestra red funciona de manera diferente respecto a lo habitual.	Se refiere a cuando nuestra red funciona de manera diferente respecto a lo habitual. Podríamos estar siendo objeto de una **infección por malware** o haber incurrido en **descuido o desconocimiento** como la falta de rutinas de mantenimiento. Algunas de las señales de funcionamiento incorrecto de la red son: •tu conexión a internet está lenta, aún tras reconocer que la capacidad de la internet contratada podría ser insuficiente para la cantidad de personas conectadas, •los dispositivos aparecen conectados a la red pero no tienen acceso a internet, •la contraseña del Wifi cambió sin que tu intervinieras (y es diferente a la que viene establecida de fábrica), no puedes acceder a recursos externos (impresoras, otras computadoras o dispositivos móviles, escáner, etc.) conectados a la red y a los que usualmente accedías. En caso de haber sido objeto de **infección dirigida** de malware se estarían violando nuestros derecho a la **privacidad y a defender derechos humanos** puesto que expone nuestra información privada y de terceros y, a través de la red, recabamos y difundimos información sobre nuestra labor.	HARDWARE

Glosario

Acoso en línea: es una práctica de agresión que busca intimidar, perseguir, e importunar a una persona defensora. Cuando se da en el entorno digital se habla de acoso en línea y esto puede ser llevado a cabo por *trolls, bots* o identidades falsas. Existen varios tipos de acoso, entre otros el acoso sexual, psicológico, laboral. El acoso sexual es una forma específica de violencia de género a menudo usada en contra de mujeres y personas de la comunidad LGBTIQ que defienden derechos humanos.

Amenaza en línea: es una práctica de agresión que se manifiesta por medio de declaraciones o comportamientos agresivos que pretenden forzarnos a realizar alguna acción a través de la promesa de un daño o un castigo en nuestra contra. Cuando se da en el entorno digital se habla de amenaza en línea y esto puede ser llevado a cabo por *trolls, bots* o perfiles específicamente creados para estos fines que complican identificar a la persona agresora. Es a menudo usada en contra de quienes defienden derechos humanos con el objetivo de disuadirnos o forzarnos a realizar alguna acción más allá de nuestra voluntad y que de otro modo no haríamos.

Ataque de denegación de servicios (DDoS): se trata de una práctica realizada para tomar control de la visualización de una página web u otro servicio en línea. El método utilizado implica coordinar la "solicitud" de la dirección web o envío de información donde se encuentra alojado el servicio produciendo un flujo de tráfico mayor al que el servidor puede responder obteniendo como resultado que ya no se pueda acceder al sitio.

Ataque de *phishing*: es una de las acciones de ingeniería social más utilizadas en medios digitales. Se trata de una técnica por la cual se envían mensajes a través de correos electrónicos, clientes de mensajería o mensajes de texto con el objetivo de que las personas ingresen sus datos personales en una página web que simula ser verídica o bien instan a descargar archivos adjuntos. A través de cualquiera de estos dos mecanismos se logra acceder directamente a cuentas o se recaba información privada de las mismas por medio de una infección por *malware* que se ejecuta en tu dispositivo.

Bot: es el diminutivo de “robot” y usualmente refiere a un *software* desarrollado para realiza tareas en línea de forma automatizada a velocidades de cómputo, es decir, que son capaces de realizar la misma o varias acciones casi al mismo tiempo. Los *bots* pueden ser diseñados tanto para publicar contenido en diversos medios y plataformas como para recoger información o hacer click en objetos de páginas web.

Censura en línea: es una práctica de agresión que busca controlar, filtrar o restringir el acceso a las comunicaciones en línea de personas o grupos y es ejercida por actores estatales con la complicidad de empresas de telecomunicaciones. Es a menudo usada en contra de quienes defienden derechos humanos para limitar su derecho de expresión.

Descuido humano: es un comportamiento individual o colectivo caracterizado por omisión, negligencia o falta de atención, que puede causarnos algún tipo de daño. En quienes defienden derechos humanos puede ser causado por desconocimiento, alta carga de trabajo, estrés o vulnerabilidad emocional.

Difamación en línea: es una práctica de agresión que busca desacreditar a una persona u organización por medio de la publicación de información falsa en páginas web, redes sociales, u otras plataformas digitales. Cuando se da en el entorno digital se habla de difamación en línea y esto puede ser llevado a cabo por trolls, botso perfiles específicamente creados para estos fines que complican identificar a la persona agresora. Es a menudo utilizada en contra de quienes defienden derechos humanos con el objetivo de provocar daño, desacreditar su trabajo, limitar el espacio de actuación, instigar a la violencia y/o justificar la criminalización en su contra.

Doxxing: se refiere a la práctica mediante la cual se monitorea y almacena información sobre una persona u organización a través de fuentes abiertas como perfiles de redes sociales, periódicos, etc. En ocasiones también pueden usarse métodos ilegales para hacerse con los datos deseados. La información recolectada es analizada con el objetivo de crear perfiles de dichas personas u organizaciones y eventualmente realizar ataques como la publicación de información confidencial, acoso, difamación, etc. Se diferencia del ciberpatrullaje principalmente en que el doxxingno es realizado por actores estatales.

Extorsión en línea: es una declaración que pretende forzarnos a realizar algo por medio de amenazas, normalmente con la finalidad de conseguir dinero. Cuando se da en el entorno digital se habla de extorsión en línea y puede ser llevado a cabo por *trolls, bots* o perfiles específicamente creados para estos fines que complican identificar a la persona agresora. Es a menudo usada en contra de quienes defienden derechos humanos con el objetivo de disuadirnos o forzarnos a realizar alguna acción más allá de nuestra voluntad y que de otro modo no haríamos.

Intimidación en línea: es una práctica de agresión que puede manifestarse con declaraciones directas o comportamientos que pretenden generar tensión, temor o miedo. Cuando se da en el entorno digital se habla de intimidación en línea y esto puede ser llevado a cabo por *trolls, bots* o perfiles específicamente creados para estos fines que complican identificar a la persona agresora. Es a menudo usada en contra de quienes defienden derechos humanos para disuadirnos de realizar alguna acción o declaración.

Key logger: se refiere a un programa informático (en muchos casos *malware*) o dispositivos físicos utilizados para grabar los golpes de teclado, es decir, registrar cada pulsación realizada en el teclado y de esta forma poder reconstruir lo que se ha escrito, desde contraseñas a textos completos que se envían automáticamente a una dirección desconocida.

Malware: en la actualidad, una creciente cantidad de *software* se escribe con fines malicioso. Se considera *malware* a todo programa diseñado para realizar acciones intrusivas no requeridas sobre otros dispositivos o *software*. Dentro de esta categoría encontramos tanto virus informáticos como programas que permitan acceder remotamente a *hardware*, copiar o borrar información, grabar o modificar contenidos. Una de las formas más comunes para la instalación de *malware* es a través de ataques de *pishing*. También pueden infectarse aquellos dispositivos a los que se tiene acceso físico.

Troll: es un término utilizado para referirse a las personas que intencionalmente realizan acciones contra otras personas con el objetivo de molestar, acosar o enviar mensajes de odio a través de plataformas digitales.

Vigilancia en línea y ciberpatrullaje: ambos términos se refieren a prácticas de agresión que buscan obtener información acerca de alguien mediante los medios digitales. En algunos casos, persiguen intimidar y/o recabar la información necesaria sobre alguien para perpetrar un ataque en su contra. Algunos Estados han implementado vigilancia en línea a través de *spywares* y otros *malwares*. Con ciberpatrullaje en particular se entiende la práctica mediante la cual actores estatales monitorean y almacenan información sobre organizaciones, activistas, periodistas y personas defensoras de derechos humanos que se encuentra accesible a través de fuentes abiertas como perfiles de redes sociales, periódicos, etc. La información recolectada es almacenada y analizada con el objetivo de crear perfiles sociales de dichos grupos. Ambas acciones están fuertemente ligadas a labores de inteligencia.

Referencias

Access Now (2019) Línea de Ayuda de Seguridad Digital. En: https://www.accessnow.org/help-es/?ignorelocale

Artículo 19, R3D, Social Tic (2017). Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México.

Barry, Jane (2011) "Manual de Seguridad Integral". En: http://www.integratedsecuritymanual.org/sites/default/files/integratedsecurity_themanual.pdf

Brigadas Internacionales de Paz (2014) "Guía de Facilitación del Programa de Asesorías en Seguridad y Protección para Personas Defensoras de Derechos Humanos". En: https://seguridadparadefender.org/sites/seguridadparadefender.org/files 2014ProgramaAsesoriasSeguridadProteccion_PBIMexico.pdf

CELS - Centro de Estudios Legales y Sociales (2017) "Reunión de la omc en la Argentina: acreditaciones rechazadas y deportaciones". En: https://www.cels.org.ar/web/2017/12/wto-meeting-in-argentina-rejected-accreditations-and-deportations/

Cibeira, Fernando (2020) "Espionaje ilegal: las fichas de la AFI de Macri y Bullrich sobre periodistas y empresarios", Página 12. En: https://www.pagina12.com.ar/270760-espionaje-ilegal-las-fichas-de-la-afi-de-macri-y-bullrich-so

CiviCert (2020) "Kit de primeros auxilios digitales". En: https://digital-firstaid.org/es/

Colectivo Ansur (2013) "Tejidos de Protección". En: https://seguridadparadefender.org/sites/seguridadparadefender.org/files/2013TejidosProteccion_ColectivoANSUR.pdf

EFF (2019) "EFF se suma a organizaciones de América Latina que se oponen a la acusación de Ola Bini". En: https://www.eff.org/deeplinks/2019/08/eff-se-suma-organizaciones-de-america-latina-que-se-oponen-la-acusacion-de-ola

EFF (s/f) "Guía de Autoprotección Digital Contra La Vigilancia". En: https://ssd.eff.org/

Flacso México y IBHARI1 (2017) "Manual de Análisis de contexto para casos de Violaciones a los Derechos Humanos". En: https://www.flacso-.edu.mx/sites/default/files/violaciones-ddhh-y-contexto-herramientas-propuestas-para-documentar-investigar.pdf

Flores-Macías, Gustavo A. (2020) Una tormenta azotará las democra cias latinoamericanas (New York Times, 15-06-2020). En: https://www.nytimes.com/es/2020/06/15/espanol/opinion/coronavirus-democracias-latinoamerica.html

Forst, M (2020) Defender y proteger a las personas defensoras de De rechos Humanos.

Front Line Defenders & Tactical Technology Collective (2011) Security in a box: Herramientas y tácticas de seguridad digital. En: https://securityinabox.org/es/

Front Line Defenders (2016) Digital Security & Privacy for Human Rights Defenders. Disponible en: https://www.frontlinedefenders.org/en/resource-publication/digital-security-privacy-human-rights-defenders

Fundación Acceso (2019) “Observatorio Centroamericano de Seguridad Digital“. En: https://acceso.or.cr/assets/files/Informe_OSD_2018_espan%CC%83ol.pdf

HACK*BLOSSOM (s/f) “Guía de Seguridad Digital para Feministas Autogestivas”. En: https://es.hackblossom.org/cybersecurity/

IM-Defensoras (2020) "El Salvador: Organizaciones preocupadas por incremento de violencia digital contra defensoras". En:
https://im-defensoras.org/2020/06/el-salvador-organizaciones-preocupadas-por-incremento-de-violencia-digital-contra-defensoras/

Internet World Stats (2020) https://internetworldstats.com/

Protección Internacional (2009) Nuevo Manual de Protección para De fensores de Derechos Humanos. En: https://www.protectioninternational.org/wp-content/uploads/2012/04/Nuevo_Manual_Proteccion.pdf

Protección Internacional Mesoamérica (2020) Cuidándonos: Guía para la Protección Colectiva de Defensoras y Defensores de Derechos Humanos en Áreas Rurales. En: https://www.protectioninternational.org/sites/default/files/cuidandonos-espanol.pdf

Sursiendo (2018) "Comunicado: Ley que regula los actos de odio y dis criminación en Internet de Honduras". En: https://sursiendo.org/blog/2018/02/comunicado-ley-que-regula-los-actos-de-odio-y-discriminacion-en-internet-de-honduras/

Sursiendo (2019a) Vigilancia Digital en México. En: https://sursiendo.org/docs/vigilancia_mexico_resumen2018.pdf

Sursiendo (2019b) "Declaración sobre la represión de la protesta social en América Latina a través de la violencia y el uso de la tecnología". En: https://sursiendo.org/blog/2019/11/declaracion-sobre-la-represion-de-la-protesta-social-en-america-latina-a-traves-de-la-violencia-y-el-uso-de-la-tecnologia/

Sursiendo (2019c) "Organizaciones de derechos humanos rechazan medidas arbitrarias contra el investigador en seguridad digital Javier Smaldone". En: https://sursiendo.org/blog/2019/11/organizaciones-de-derechos-humanos-rechazan-medidas-arbitrarias-contra-el-investigador-en-seguridad-digital-javier-smaldone/

Sursiendo (2020) "Proyecto de ley de desinformación brasileño amenaza la libertad de expresión y la privacidad en línea". En: https://sursiendo.org/blog/2020/06/proyecto-de-ley-de-desinformacion-brasileno-amenaza-la-libertad-de-expresion-y-la-privacidad-en-linea/

Tactical Technology Collective (2015) "Zen y el arte de que la tecnología trabaje para ti". En: https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es

Tactical Techonolgy Collective (2016) “Manual de Seguridad Holística”. En: https://holistic-security.tacticaltech.org/ckeditor_assets/attachments/61/hs_complete_hires.pdf

Tactical Technology Collective y Front Line Defenders (2011) “Security in a Box”. En: https://securityinabox.org/es/

Técnicas Rudas (2018) “Mapeo de Información”. En: https://es.gendersec.train.tacticaltech.org

The Engine Roome (2018) Lazos que unen. Seguridad organizacional para la sociedad civil. Disponible en: https://www.theengineroom.org/wp-content/uploads/2018/03/Lazos-que-unen-Seguridad-organizacional-para-la-sociedad-civil.pdf

The Intercept Brasil Live (2020) "PL de fake news e outras ideias ruins_Tatiana Dias com Bruna Martins". Podcast en: https://open.spotify.com/episode/1JPqifDpt3GpUXWDtrA4SB?si=xAHkoVljQdGimBy9plR5RQ

Wikipedia (2019) Operación Huracán. En: https://es.wikipedia.org/wiki/Operaci%C3%B3n_Hurac%C3%A1n

Esta investigación se realizó y diseñó con software libre: LibreOffice, Inkscape, Gimp y Scribus. Se usaron las fuentes tipográficas libres "Cantarell" en 9 puntos para el cuerpo del texto y "Coustard" en 20 puntos para los títulos.

Esta publicación se imprimió en La Cosecha, en octubre de 2020
San Cristóbal de Las Casas, Chiapas, México.

